TANDBERG

VIDEO COMMUNICATION SERVER

ADMINISTRATOR GUIDE



Software version X1.0
D14049.01
July 2007

TANDBERG
VIDEO COMMUNICATION SERVER

What's in this ADMINISTRATOR GUIDE?

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Trademarks and Copyright

Philip Pedersens vei 22
1366 Lysaker, Norway
Tel: +47 67 125 125
Fax: +47 67 125 234
e-mail: tandberg@tandberg.com

Disclaimer, Copyrights and License Agreements

Disclaimer

The information in this document is furnished for informational purposes only, is subject to change without prior notice, and should not be construed as a commitment by TANDBERG.

TANDBERG reserves the right to amend any of the information given in this document in order to take account of new developments.

Every effort has been made to supply complete and accurate information, however, TANDBERG assumes no responsibility or liability for any errors or inaccuracies that may appear in this document, nor for any infringements of patents or other rights of third parties resulting from its use. No license is granted under any patents or patent rights of TANDBERG.

Copyright Notice

Tandberg software in this product is protected under the copyright and patent laws.

Patents pending in the U.S.

This product includes copyrighted software licensed from others. A list of the copyright notices and the terms and conditions of use can be found at:

http://www.tandberg.com/collateral/documentation/User_Manuals/TANDBERG VCS EULA.pdf

and

http://www.tandberg.com/collateral/documentation/User_Manuals/TANDBERG VCS Copyrights.pdf.

IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.

Patent Information

TANDBERG technology described in this manual is protected by one or more of the following:

U.S. Patent Nos.

- 5,600,646
- 5,768,263
- 5,838,664
- 5,991,277
- 6,584,077
- 6,590,603
- 7,010,119
- 7,034,860

U.S. Patent Application Nos.

- 10/332.785
- 10/432.468
- 11/008.150

Other patents pending.

Safety Instructions and Approvals

Safety Instructions

For your protection please read these safety instructions completely before you connect the equipment to the power source. Carefully observe all warnings, precautions and instructions both on the apparatus and in these operating instructions. Retain this manual for future reference.

Water and Moisture

- Do not operate the apparatus under or near water – for example near a bathtub, kitchen sink, or laundry tub, in a wet basement, near a swimming pool or in other areas with high humidity.
- Never install jacks for communication cables in wet locations unless the jack is specifically designed for wet locations.
- Do not touch the product with wet hands.

Cleaning

- Unplug the apparatus from communication lines, mains power-outlet or any power source before cleaning or polishing.
- Do not use liquid cleaners or aerosol cleaners. Use a lint-free cloth lightly moistened with water for cleaning the exterior of the apparatus.

Ventilation

- Do not block any of the ventilation openings of the apparatus. Never cover the slots and openings with a cloth or other material. Never install the apparatus near heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
- Do not place the product in direct sunlight or close to a surface directly heated by the sun.

Lightning

Never use this apparatus, or connect/disconnect communication cables or power cables during lightning storms.

Dust

Do not operate the apparatus in areas with high concentration of dust.

Vibration

Do not operate the apparatus in areas with vibration or place it on an unstable surface.

Power Connection and Hazardous Voltage

- The product may have hazardous voltage inside. Never attempt to open this product, or any peripherals connected to the product, where this action requires a tool.
- This product should always be powered from an earthed power outlet.
- Never connect attached power supply cord to other products.
- In case any parts of the product has visual damage never attempt to connect mains power, or any other power source, before consulting service personnel
- The plug connecting the power cord to the product/power supply serves as the main disconnect device for this equipment. The power cord must always be easily accessible.
- Route the power cord so as to avoid it being walked on or pinched by items placed upon or against it. Pay particular attention to the plugs, receptacles and the point where the cord exits from the apparatus.
- Do not tug the power cord.
- If the provided plug does not fit into your outlet, consult an electrician.
- Never install cables, or any peripherals, without first unplugging the device from it's power source.

Servicing

- Do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.
- Unplug the apparatus from its power source and refer servicing to qualified personnel under the following conditions:
  - If the power cord or plug is damaged or frayed.
  - If liquid has been spilled into the apparatus.
  - If objects have fallen into the apparatus.
  - If the apparatus has been exposed to rain or moisture
  - If the apparatus has been subjected to excessive shock by being dropped.
  - If the cabinet has been damaged.
  - If the apparatus seems to be overheated.
  - If the apparatus emits smoke or abnormal odor.
  - If the apparatus fails to operate in accordance with the operating instructions.

Accessories

Use only accessories specified by the manufacturer, or sold with the apparatus.

Approvals

Electromagnetic Compatibility (EMC)

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

EC Declaration of Conformity

Manufacturer: TANDBERG Telecom AS

Product Name: TANDBERG Video Communication Server

Type Number: TTC2-04

Description: Network unit

This product complies with Commission Directives:

- LVD 73/23/EEC
- EMC 89/336/EEC

This product complies with harmonized Standards:

- EN 60950-1 : 2001, A11
- EN 55022 : 1994, A1/A2
- EN 55024 : 1998, A1/A2
- EN 61000-3-2 : 2000
- EN 61000-3-3 : 1995, A1

Technical Construction File No.: X13526

Year which the CE mark was affixed: 2007

For an official, signed version of this document, or details regarding documentation from the technical construction file, please contact TANDBERG.

JATE Approval (Japan only)

This unit must be connected to the public internet via a router/switch that has JATE approval.

Environmental Issues

Thank you for buying a product which contributes to a reduction in pollution, and thereby helps save the environment. Our products reduce the need for travel and transport and thereby reduce pollution. Our products have either none or few consumable parts (chemicals, toner, gas, paper). Our products are low energy consuming products.

TANDBERG's Environmental Policy

Environmental stewardship is important to TANDBERG's culture. As a global company with strong corporate values, TANDBERG is committed to following international environmental legislation and designing technologies that help companies, individuals and communities creatively address environmental challenges.

TANDBERG's environmental objectives are to:

- Develop products that reduce energy consumption, CO_2 emissions, and traffic congestion
- Provide products and services that improve quality of life for our customers
- Produce products that can be recycled or disposed of safely at the end of product life
- Comply with all relevant environmental legislation.

European Environmental Directives

As a manufacturer of electrical and electronic equipment TANDBERG is responsible for compliance with the requirements in the European Directives 2002/96/EC (WEEE) and 2002/95/EC (RoHS).

The primary aim of the WEEE Directive and RoHS Directive is to reduce the impact of disposal of electrical and electronic equipment at end-of-life. The WEEE Directive aims to reduce the amount of WEEE sent for disposal to landfill or incineration by requiring producers to arrange for collection and recycling. The RoHS Directive bans the use of certain heavy metals and brominated flame retardants to reduce the environmental impact of WEEE which is landfilled or incinerated.

TANDBERG has implemented necessary process changes to comply with the European RoHS Directive (2002/95/EC) and the European WEEE Directive (2002/96/EC).

Waste Handling

In order to avoid the dissemination of hazardous substances in our environment and to diminish the pressure on natural resources, we encourage you to use the appropriate take-back systems in your area. Those systems will reuse or recycle most of the materials of your end of life equipment in a sound way.



TANDBERG products put on the market after August 2005 are marked with a crossed-out wheelie bin symbol that invites you to use those take-back systems.

Please contact your local supplier, the regional waste administration, or http://www.tandberg.com/recycling if you need more information on the collection and recycling system in your area.

Information for Recyclers

As part of compliance with the European WEEE Directive, TANDBERG provides recycling information on request for all types of new equipment put on the market in Europe after August 13th 2005.

Please contact TANDBERG and provide the following details for the product for which you would like to receive recycling information:

- Model number of TANDBERG product
- Your company's name
- Contact name
- Address
- Telephone number
- E-mail.

Digital User Guides

TANDBERG is pleased to announce that we have replaced the printed versions of our User Guides with a digital CD version. Instead of a range of different user manuals, there is now one CD – which can be used with all TANDBERG products – in a variety of languages. The environmental benefits of this are significant. The CDs are recyclable and the savings on paper are huge. A simple web-based search feature helps you directly access the information you need. In addition, the TANDBERG video systems now have an intuitive on-page help function, which provides a range of useful features and tips. The contents of the CD can still be printed locally, whenever needed.

Environmental Issues

产品中有毒有害物质表

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
金属部件	X	O	O	O	O	O
印刷电路板及组件	X	O	O	O	O	O
线缆和线缆组装	X	O	O	O	O	O
显示器（包括照明灯）	X	X	O	O	O	O

说明:

O：表示该有毒有害物质在此部件所有均质材料中的含量均在中国标准《电子信息产品中有毒有害物质的限量要求》(SJ/T 11363-2006) 所规定的限量要求以下。

X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出中国标准《电子信息产品中有毒有害物质的限量要求》(SJ/T 11363-2006) 所规定的限量要求。

注意：在所售产品中未必包含所有上述所列部件。

除非在产品上有另外特别的标注，以下标志为针对所涉及产品的环保使用期限标志。环保使用期限只适用于产品在产品手册中所规定的使用条件。

Introduction

About the TANDBERG Video Communication Server

The TANDBERG Video Communication Server (VCS) is a key component of your video communications network. It allows you to manage endpoint registrations and calls, and control the bandwidth being used within your network. The VCS also offers advanced call policy that allows you to accept, reject and re-route calls, and can optionally include TANDBERG's FindMe™, which allows users to have a single alias on which they can be contacted regardless of location,

The VCS forms part of TANDBERG's Expressway™ firewall traversal solution, allowing you to securely connect to other video networks and equipment from your secured private network.

The VCS also acts as a gateway between SIP and H.323 protocols, and between IPv4 and IPv6, allowing you to make the most use of your existing video communications investment.

Main Product Features

Standard Features

- H.323 gatekeeper
- SIP Proxy/Registrar
- SIP and H.323 support, including SIP/H.323 gatewaying for locally registered endpoints
- IPv4 and IPv6 support, including IPv4/IPv6 gatewaying
- Bandwidth management on both a per-call and a total usage basis, configurable separately for calls within the local subzones and to neighboring systems and zones
- Automatic downspeeding option for calls that exceed the available bandwidth
- URI and ENUM dialing via DNS, enabling global connectivity
- Up to 2500 registrations
- Up to 500 non-traversal calls
- Up to 100 traversal calls
- Up to 200 neighboring zones
- Flexible zone configuration with prefix, suffix and regex support
- Can function as a stand-alone VCS or be neighbored with other systems such as VCSs, Border Controllers, gatekeepers and SIP proxies
- Supports up to 5 Alternate VCSs for redundancy purposes
- Optional endpoint authentication
- Control over which endpoints are allowed to register
- Administrator Policy including support for CPL
- Embedded setup wizard via a serial port for initial configuration
- System administration via a web interface or RS-232, Telnet, SSH, and HTTPS
- Can be managed with TANDBERG Management Suite 11.8 or newer

Optional Features

- Firewall traversal server functionality, allowing secure traversal of any firewall or NAT
- Registration of traversal-enabled endpoints
- STUN Discovery and STUN Relay services
- User Policy (TANDBERG FindMe™)
- SIP/H.323 gatewaying for non-registered endpoints

About this Administrator Guide

This Administrator Guide is provided to help you make the best use of your TANDBERG VCS.

Your approach to this documentation depends on what you want to do and how much you already know.

The Administrator Guide has been divided into several sections, each providing different information. In some places information is duplicated between sections to let you have all the relevant information in one place.

This document does not have an index - this is intentional. If the Table of Contents does not direct you to the information you need, you can use the Find function in Adobe Reader to search the text for keywords.

Note that the Administrator Guide describes a fully equipped version. Your version may not have all the described extensions installed.

Our main objective with this Guide is to address your goals and needs. Please let us know how well we succeeded!

In this Administrator Guide, instructions for performing a task via the web interface are shown in the format:

- *Menu option1 > Menu option2*

followed by the Name of the page that you will be taken to. In most cases the page will be shown adjacent, with callouts describing each of the configurable options.

In this Administrator Guide, instructions for performing a task using the command line interface are shown in the format:

- `xConfiguration CommandName`

The command is hyperlinked to the Command Reference table at the back of this Guide; clicking on the hyperlink will take you to the appropriate section of the table showing all the available sub-commands and parameters.

Typing the command into the CLI without any parameters will return a full list of parameters available for that command.

Typing a ? after the command will return information about the purpose of that command or group of commands.

Getting Started

What's in the Box?

To avoid damage to the unit during transportation, the TANDBERG VCS is delivered in a special shipping box, which should contain the following components:

- TANDBERG VCS
- CD containing VCS Administrator Guide and other documentation
- Installation Sheet
- Registration card
- Rack-ears and screws
- Cables:
  - power cables
  - ethernet cable
  - shielded serial cable

Please report discrepancies to your TANDBERG representative immediately.



A brief yet detailed description of the procedure to get you up and going can be found in the Installation Sheet accompanying your TANDBERG product.

Installation Site Preparations

- Make sure that the VCS is accessible and that all cables can be easily connected.
- For ventilation: leave a space of at least 10cm (4 inches) behind the VCS's rear panel and 10cm (4 inches) in front of the front panel.
- The room in which you install the VCS should have an ambient temperature between 0°C and 35°C (32°F and 95°F) and between 10% and 90% non-condensing relative humidity.
- Do not place heavy objects directly on top of the VCS.
- Do not place hot objects directly on top, or directly beneath the VCS.
- Use a grounded AC power outlet for the VCS.

General Installation Precautions

- The socket outlet shall be installed near to the equipment and shall be easily accessible.
- Never install cables without first switching the power OFF.

Connecting the Cables

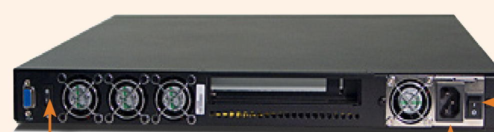


Shielded serial cable

To control the VCS using a direct connection to a PC, connect the serial cable between the VCS's DATA port and the COM port on a PC.

Ethernet cable.

To use the VCS over IP, connect the ethernet cable from the LAN1 port on the VCS to your network. The LAN2, 3 and 4 connectors are not used and should be left open.



Power switch

Soft power button

Power cable

Connect the system power cable to an electrical distribution socket.

Getting Started

Powering on the VCS

To start the VCS:

1. Ensure the power cable is connected.
2. Ensure the LAN cable is connected to the LAN1 port.
3. Turn on the power switch on the back right of the unit (adjacent to the power cable).
4. Press the soft power button on the back left of the unit.

The system will start up and the lights on the front of the unit will flash.

5. Wait until:
   - the green PWR LED on the front of the unit is a steady green color
   - the red ALM LED on the front of the unit has gone out.
   - the IP address is showing in the display panel on the front of the unit.

Once this has happened, the system is ready to configure.

Initial Configuration via Serial Cable

The VCS requires some initial configuration before it can be used. This must be done using a PC connected to the DATA port or by connecting to the system's default IP address: 192.168.0.100.

The IP address, subnet mask and default gateway must be configured before use. Consult your network administrator for information on which addresses to use. Note that the VCS must use a static IP address.

To set the initial configuration via a PC connected to the DATA port:

1. Connect the supplied serial cable from the DATA port on the VCS to the COM port on a PC.
2. Start a terminal emulator program on the PC and configure it to use the DATA port as follows:
   - baud rate 115200
   - data bits: 8
   - parity: none
   - stop bits: 1
   - flow control: none.
3. Power on the unit (if it is not already on).

   The terminal emulator program will display start up information.

   After approximately 2 minutes you will get the login prompt (if the unit is already on, press Enter to get the login prompt):

   `tandberg login:`
4. Enter the username admin and press Enter.

   You will get the password prompt:

   `Password:`
5. Enter the default password of TANDBERG and press Enter.

   You will get the install wizard prompt:

   `Run install wizard [n]:`

   Type `y` and press Enter.
6. Follow the prompts given by the install wizard to specify the following:
   a. The password you want to use for your system. See Administrator Account Password for details.
   b. Whether you wish to use IPv4 or IPv6. See IP Protocol for details.
   c. The IP address of the system.
   d. The IP subnet mask of the system.
   e. The IP default gateway of the system.
   f. The ethernet speed.
   g. Whether you want to use SSH to administer the system.
   h. Whether you want to use Telnet to administer the system.
8. Once the wizard is finished you will be prompted to log in again.

   Login with the username admin and your new password.
9. You will again get the install wizard prompt; this time select `n` and press Enter in order to skip the wizard.

   A welcome message similar to the following will appear:

   ```
   Welcome to
   TANDBERG Video Communication
   Server Release X1.0
   SW Release Date: 2007-07-20
   OK
   ```
10. You must now reboot the system in order for the new settings take effect. To do this, type the command:

    `xCommand boot`

Once it has rebooted, the VCS is ready to use. You can continue to use the serial connection, or you can connect to the system remotely over IP using either or both:

- the web interface via HTTPS
- a command line interface via SSH or Telnet.

We recommend that you now configure the following:

- The system name of the VCS. This is used by the TANDBERG Management Suite (TMS) to identify the system. See About the System Name for more information.
- Automatic discovery. If you have multiple VCSs in the same network you may want to disable automatic discovery on some of them. See Auto Discover for more information.
- The DNS server address (if URI dialing or FQDNs are to be used). See DNS configuration for more information.

System Administrator Access

About Administrator Access

While it is possible to administer the TANDBERG VCS via a PC connected directly to the unit via a serial cable, you may wish to access the system remotely over IP.

You can do this using either or both:

- the web interface via HTTPS
- a command line interface via SSH or Telnet.

By default, access via HTTPS and SSH is enabled; access via Telnet is disabled.

You can also enable access via HTTP. However, this mode works by redirecting HTTP calls to the HTTPS port, so HTTPS must also be enabled for access via HTTP to function.

TMS accesses the VCS via the web server. If HTTPS mode is turned off, TMS will not be able to access it.

Configuring Administrator Access

To configure the ways in which your system is accessed:

- *System Configuration > System*.
  You will be taken to the System Administration page.
  In the Admin Access section, select Off or On from the drop-down boxes for each service.
- `xConfiguration Administration`

You must restart the system for changes to take effect.

Security Considerations

To securely manage the VCS you should disable Telnet, using the encrypted HTTPS and SSH protocols instead.

For further security, disable HTTPS and SSH as well and use the serial port to manage the system.

Administrator Account Password

All administration requires you to log in to the administration account with the username admin (all lower case) and a password.

Both the username and password are case-sensitive.

Default Administrator Password

The default password is TANDBERG (all upper case). You should change this as soon as possible. Choose a strong password, particularly if administration over IP is enabled.

Changing the Administrator Password

To change the administrator password:

- *Maintenance > Passwords.*
  You will be taken to the Passwords page.
  In the Administrator Password section, enter and then retype the new password.
- `xConfiguration SystemUnit Password`

To set an empty password type:

`xConfiguration SystemUnit Password: ""`

Resetting the Administrator Password

If you forget your password, it is possible to set a new password using the following procedure:

1. Reboot the VCS.
2. Connect to the VCS using the serial cable.
3. Login with the username pwrec. No password is required.

You will be prompted for a new password.

The pwrec account is only active for one minute following a restart. Beyond that time you will have to restart the system again to change the password.

Because access to the serial port allows the password to be reset, it is recommended that you install the VCS in a physically secure environment.

Session Timeout

By default, Administrator sessions do not time out – they remain active until you logout.

However, you can set the system to timeout an Administrator session after a set number of minutes of inactivity. The timeout period will apply to Administrator sessions using both the Web Interface and the Command Line Interface.

To set the timeout period:

- *System Configuration > System*.
  You will be taken to the System Administration page.
  In the Admin Access section, in the Session time out (minutes) box, enter the number of minutes of inactivity after which an administrator session should time out.
- `xConfiguration Administration TimeOut`

Values must be between 0 and 10,000. A value of 0 means that Administrator sessions will never time out.

You must restart the system for changes to take effect.

Root Account

The VCS provides a root account with the same password as the Admin account. This account should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the admin account instead.

System Administrator Access

Using the Web Interface

To use the web interface:

1. Open a browser window and in the address line type either:
   - the IP address of the system
   - the FQDN of the system.
2. Select Administrator Login.
3. Enter the Username admin and your system password and select Login.

You will be presented with the Overview page.

Supported Browsers

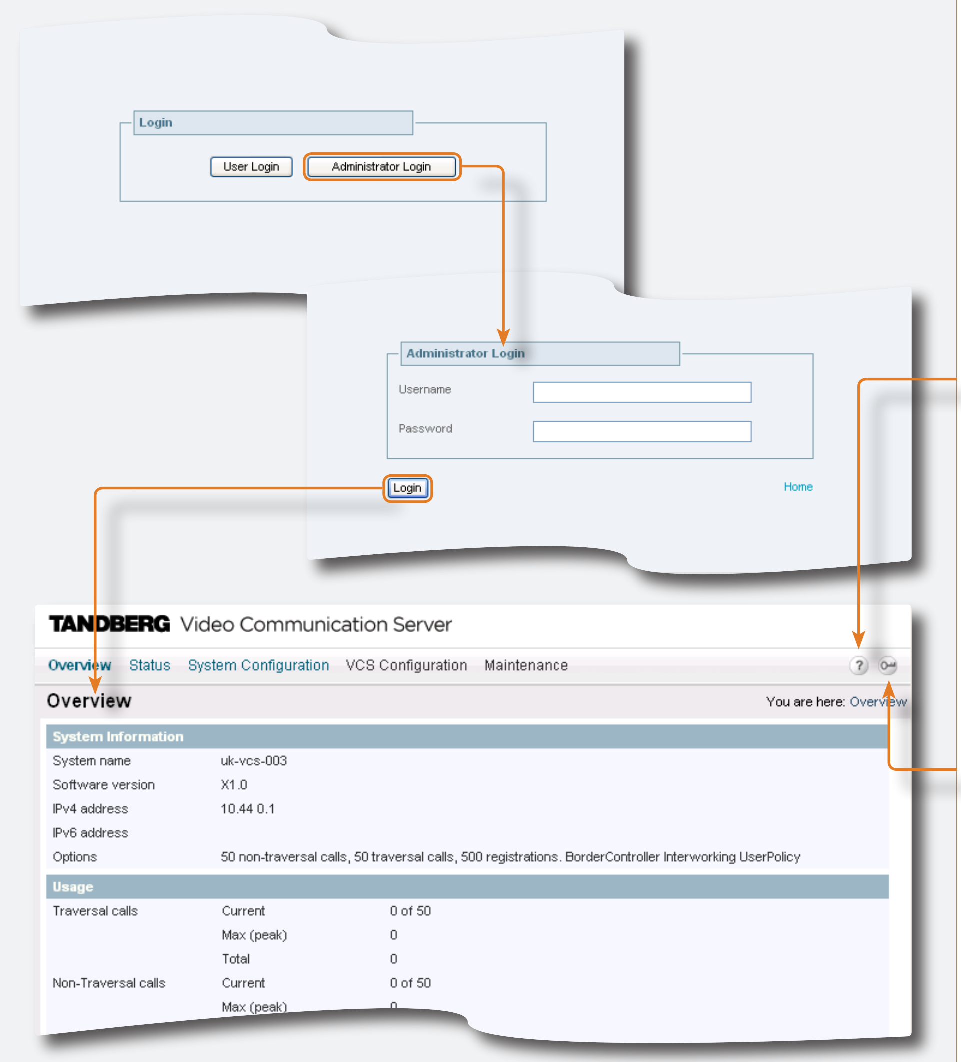
The VCS web interface is designed for use with Internet Explorer (6 and up) or Firefox (1.5 and up). It may work with Opera and Safari, but you may encounter unexpected behavior.

Javascript must be enabled to use the VCS web interface.

In this Administrator Guide, instructions for performing a task via the web interface are shown in the format:

- *Menu option1 > Menu option2*

followed by the Name of the page that you will be taken to in order to perform the task. In most cases the page will be shown adjacent with callouts describing each of the configurable options.



Information

This icon appears to the right of most input fields in the web interface.

Clicking on this icon will activate a pop-up box which gives you information about that particular field.

View manual

This icon appears on the top right corner of every screen.

Clicking on this icon will take you directly to the latest version of the VCS Administrator Guide on the TANDBERG website.

Log out

This icon appears on the top right corner of every page.

Clicking on this icon will end your Administrator session. You will be taken to the Administrator Login page.

System Administrator Access

Using the Command Line Interface (CLI)

The command line interface is available over SSH, Telnet and through the serial port.

To use the command line interface:

1. Start a SSH or Telnet session.
2. Enter the IP address or FQDN of the VCS.
3. Login with a username of admin and your system password.

Commands are divided into different groups according to their function:

xStatus	These commands return information about the current status of the system. Information such as current calls and registrations is available through this command group.
xConfiguration	These commands allow you to add and edit single items of data such as IP address and zones.
xCommand	These commands allow you to add and configure items and obtain information.
xHistory	These commands provide historical information about calls and registrations.
xFeedback	These commands provide information about events as they happen, such as calls and registrations.

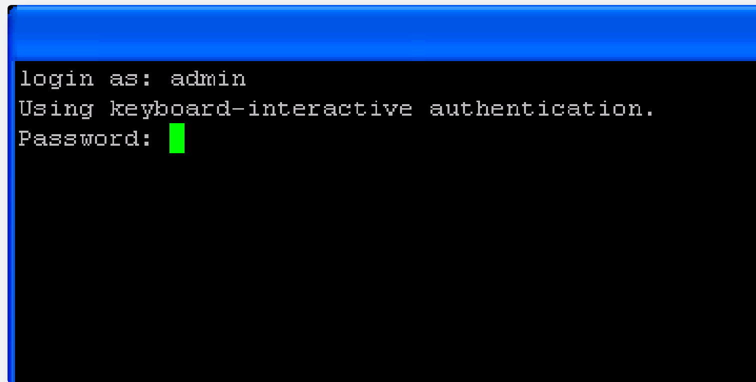
See the Command Reference Appendix for a full description of commands available on the VCS.

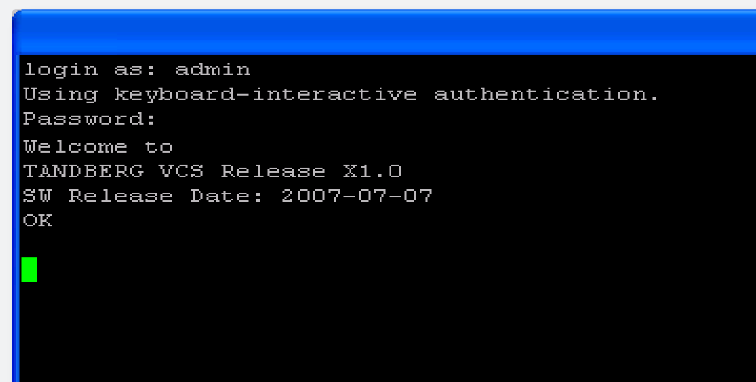
In this Administrator Guide, instructions for performing a task using the command line interface are shown in the format:

- `xConfiguration CommandName`

Typing the given command into the CLI will return a full list of options and parameters available for that command.

Typing a ? after the command will return information about the purpose of that command or group of commands.





Viewing System Overview

Viewing the Overview Page

The Overview page summarizes the current configuration and status of your system.

The Overview page opens automatically when you first log on to the web interface.

You can also access it at any time by clicking on the Overview link at the top left of the page.

System name

This shows the name that has been assigned to the VCS.

Software version

This shows the version of software that is currently installed on the VCS.

IPv4 address

This shows the VCS's IPv4 address.

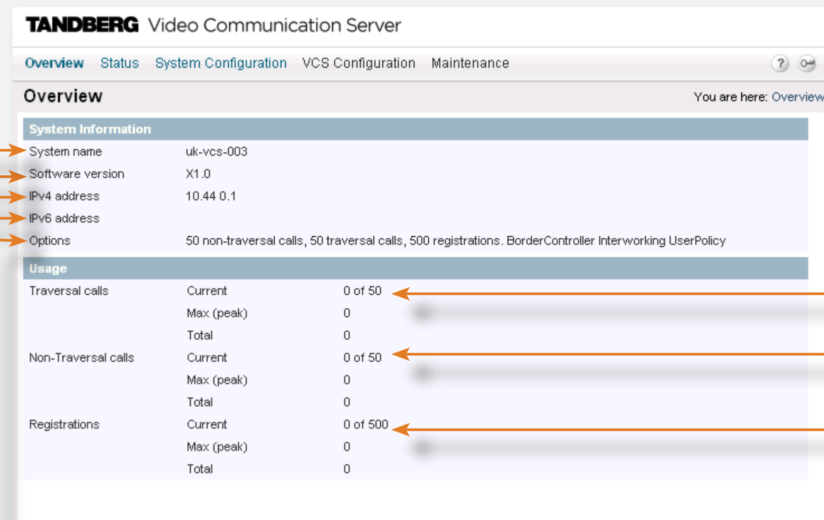
IPv6 address

This shows the VCS's IPv6 address.

Options

This shows all the additional options that are currently installed on the VCS.

Understanding the Overview Page



Traversal calls

Current: The number of traversal calls going through the VCS at this moment.

Max (peak): The highest number of concurrent traversal calls handled by the VCS since it was last restarted.

Total: The total number of traversal calls handled by the VCS since it was last restarted.

Non-traversal calls

Current: The number of non-traversal calls going through the VCS at this moment.

Max (peak): The highest number of concurrent non-traversal calls handled by the VCS since it was last restarted.

Total: The total number of non-traversal calls handled by the VCS since it was last restarted.

Registrations

Current: The number of endpoints registered to the VCS at this moment.

Max (peak): The highest number of endpoints concurrently registered to the VCS since it was last restarted.

Total: The total number of registrations on the VCS since it was last restarted.

System Configuration

System Administration Configuration

Configuring System Settings

To configure the VCS's system administration settings:

- *System Configuration > System*.
  You will be taken to the System Administration page.
- `xConfiguration SystemUnit Name`
- `xConfiguration Administration`

About the System Name

The system name is used to identify the VCS, for example in TMS.

It appears in various places in the web interface, and in the display on the front panel of the unit, so that you can identify it when it is in a rack with other boxes. If no name is specified, these fields/display will be blank.

We recommend that you give the VCS a name that allows you to easily and uniquely identify it.

About Admin Access settings

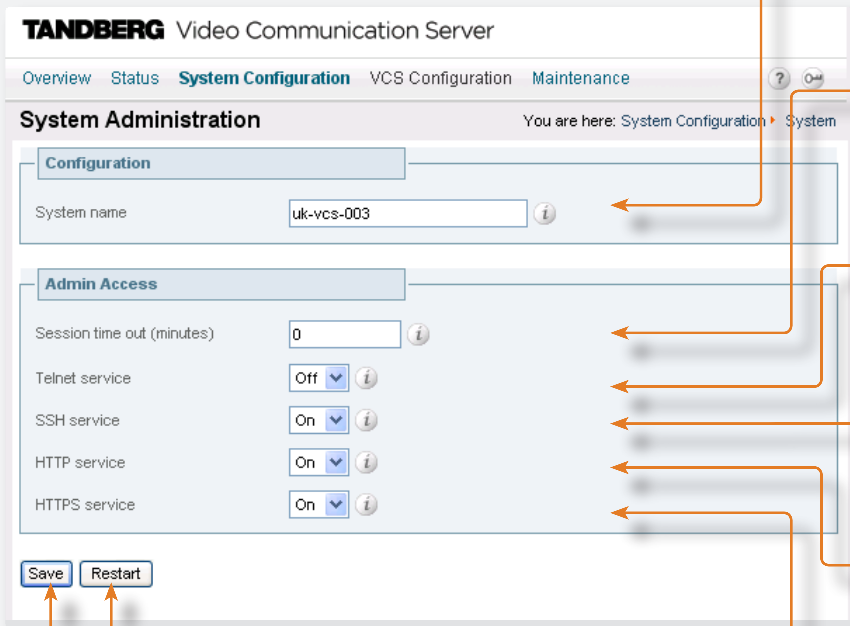
While it is possible to administer the TANDBERG VCS via a PC connected directly to the unit via a serial cable, you may wish to access the system remotely over IP.

You can do this using either or both:

- the web interface via HTTPS
- a command line interface via SSH or Telnet.

By default, access via HTTPS and SSH is enabled; access via Telnet is disabled.

You can also enable access via HTTP. However, this mode works by redirecting HTTP calls to the HTTPS port, so HTTPS must also be enabled for access via HTTP to function.



System name

Defines the name of the VCS. Choose a name that uniquely identifies the system.

Session time out (minutes)

Sets the number of minutes that an administration session (HTTPS, Telnet or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off.

Telnet service

Determines whether the VCS can be accessed via Telnet.

SSH service

Determines whether the VCS can be accessed via SSH and SCP.

HTTP service

Determines whether HTTP calls will be redirected to the HTTPS port.

HTTPS service

Determines whether the VCS can be accessed via the web server. This must be On to enable both web interface and TMS access.

Save

Click here to save your changes.

Restart

Click here to restart the system.

You must save your changes and restart the system for changes to take effect.

TMS accesses the VCS via the web server. If HTTPS mode is turned off, TMS will not be able to access it.

By default, access via HTTPS and SSH is enabled; access via Telnet is disabled. To securely manage the VCS you should disable Telnet, using the encrypted HTTPS and SSH protocols instead. For further security, disable HTTPS and SSH as well and use the serial port to manage the system.

Ethernet Configuration

Configuring Ethernet Settings

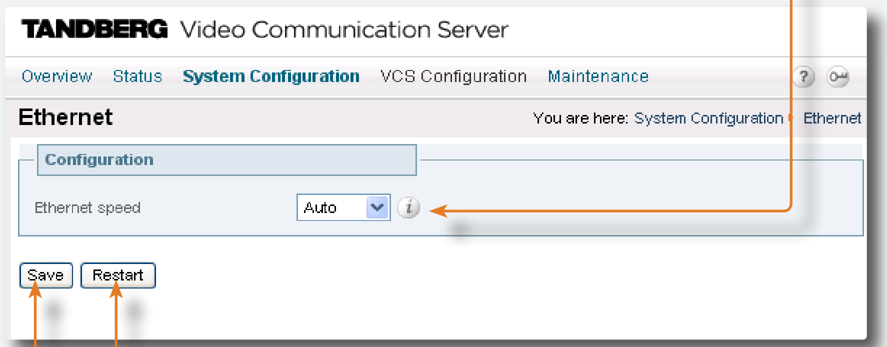
To configure the VCS's Ethernet settings:

- *System Configuration >Ethernet*.
  You will be taken to the Ethernet page.
- `xConfiguration Ethernet`

About Ethernet Speed

The Ethernet speed setting determines the speed of the connection between the VCS and the ethernet switch. It must be set to the same value on both systems.

The default is Auto. We recommend that you do not change the default value unless the switch to which you are connecting is unable to auto-negotiate.



Ethernet speed

Sets the speed of the connection between the VCS and the ethernet switch.

You must save your changes and restart the system for changes to take effect.

Restart

Click here to restart the system.

Save

Click here to save your changes.

IP Configuration

Configuring IP Settings

To configure the VCS's IP settings:

- *System Configuration > IP*.
  You will be taken to the IP page.
- xConfiguration IP
- xConfiguration IPProtocol

The VCS is shipped with a default IP address of 192.168.0.100. This allows you to connect the VCS to your network and access it via the default address so that you can configure it remotely.

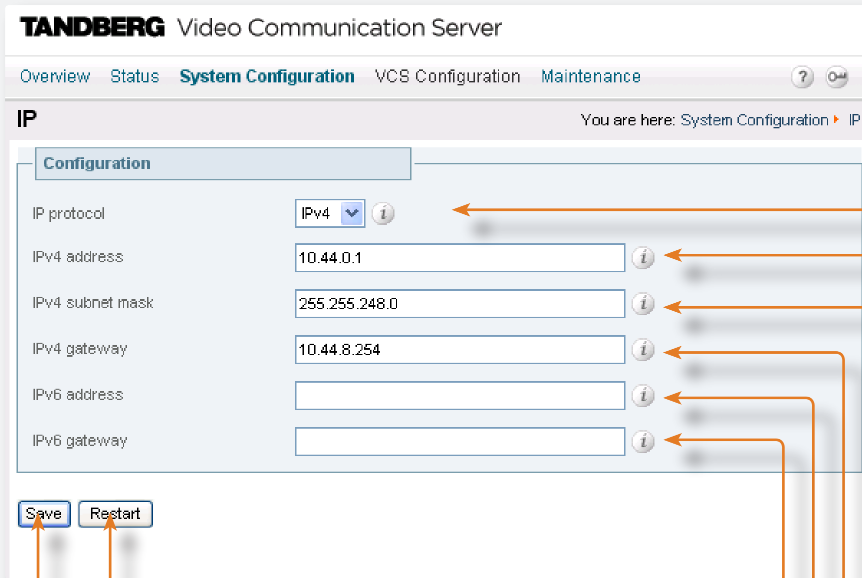
About IPv4 to IPv6 Gatewaying

The VCS can act as a gateway between IPv4 and IPv6 calls.

To configure the VCS to act as a gateway between the two protocols, select an IP Protocol of Both.

Calls for which the VCS is acting as an IPv4 to IPv6 gateway count as traversal calls for the purposes of licensing.

Some endpoints support both IPv4 and IPv6, however an endpoint can use only one protocol when registering with the VCS. Which protocol it uses will be determined by the format used to specify the IP address of the VCS on the endpoint. Once the endpoint has registered using one protocol, calls to it from an endpoint using the other protocol will be gatewayed by the VCS.



IP protocol

You can configure the VCS to use IPv4, IPv6 or Both protocols. The default is Both.

IPv4: The VCS will only accept registrations from endpoints using an IPv4 address, and will only take calls between two endpoints communicating via IPv4. It will communicate with other systems via IPv4 only.

IPv6: The VCS will only accept registrations from endpoints using an IPv6 address, and will only take calls between two endpoints communicating via IPv6. It will communicate with other systems via IPv6 only.

Both: The VCS will accept registrations from endpoints using either an IPv4 or IPv6 address, and will take calls using either protocol. If a call is between an IPv4-only and an IPv6-only endpoint, the VCS will act as an IPv4 to IPv6 gateway. It can communicate with other systems via either protocol.

IPv4 address

Specifies the IPv4 address of the system.

IPv4 subnet mask

Specifies the IPv4 subnet mask of the system.

IPv4 gateway

Specifies the IPv4 gateway of the system.

IPv6 address

Specifies the IPv6 address of the system.

You must save your changes and restart the system for changes to take effect.

Save

Click here to save your changes.

Restart

Click here to restart the system.

IPv6 gateway

Specifies the IPv6 gateway of the system.

DNS Configuration

Configuring DNS Settings

To configure the VCS's DNS settings:

- *System Configuration > DNS*.
  You will be taken to the DNS page.
- `xConfiguration IP DNS`

About DNS Servers

In order to use URI dialing or ENUM dialing, you must specify a DNS server to be queried for address resolution. You can specify up to 5 DNS servers. Normally only the first DNS server will be queried, but if it fails to respond, all DNS servers will be queried.

About the DNS Domain Name

The DNS Domain Name is used when attempting to resolve server addresses configured on the VCS that are not fully qualified. It applies only to the following:

- LDAP server
- NTP server
- External Manager server.

The DNS Domain Name is appended to the server address before a query to the DNS server is executed. Note however that DNS will also be queried for the server address as configured, without the DNS Domain Name appended. For this reason we recommend that all server addresses use a FQDN.

The DNS Domain name plays no part in URI dialing.



Address 1 to Address 5

Sets the IP address of a DNS server to be queried when resolving domain names.

Domain name

Specifies the name to be appended to the host name before a query to the DNS server is executed.

Save

Click here to save your changes.

System Configuration

NTP Configuration

Configuring NTP Settings

To configure the VCS's NTP settings:

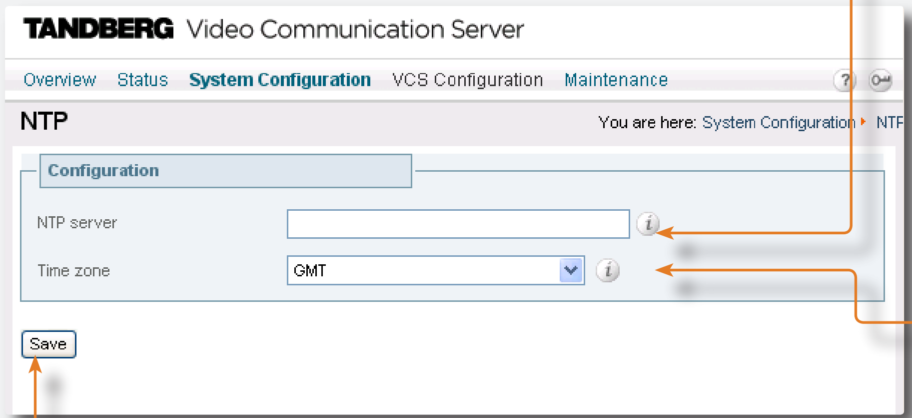
- *System Configuration > NTP*
  You will be taken to the NTP page.
- `xConfiguration NTP Address`
- `xConfiguration TimeZone Name`

About the NTP Server

Accurate timestamps play an important part in authentication, helping to guard against replay attacks. For this reason, we recommend that you use an NTP server to synchronize the system time.

Setting the Time Zone

All events are recorded using the local date and time as well as UTC time. The local time is determined by the Time Zone set on the VCS.



NTP server

Sets the IP address or FQDN of the NTP server to be used when synchronizing system time.

Time zone

Sets the local time zone of the VCS.

Save

Click here to save your changes.

SNMP Configuration

Configuring SNMP Settings

To configure the VCS's SNMP settings:

- *System Configuration > SNMP*
  You will be taken to the SNMP page.
- `xConfiguration SNMP`

About SNMP Settings

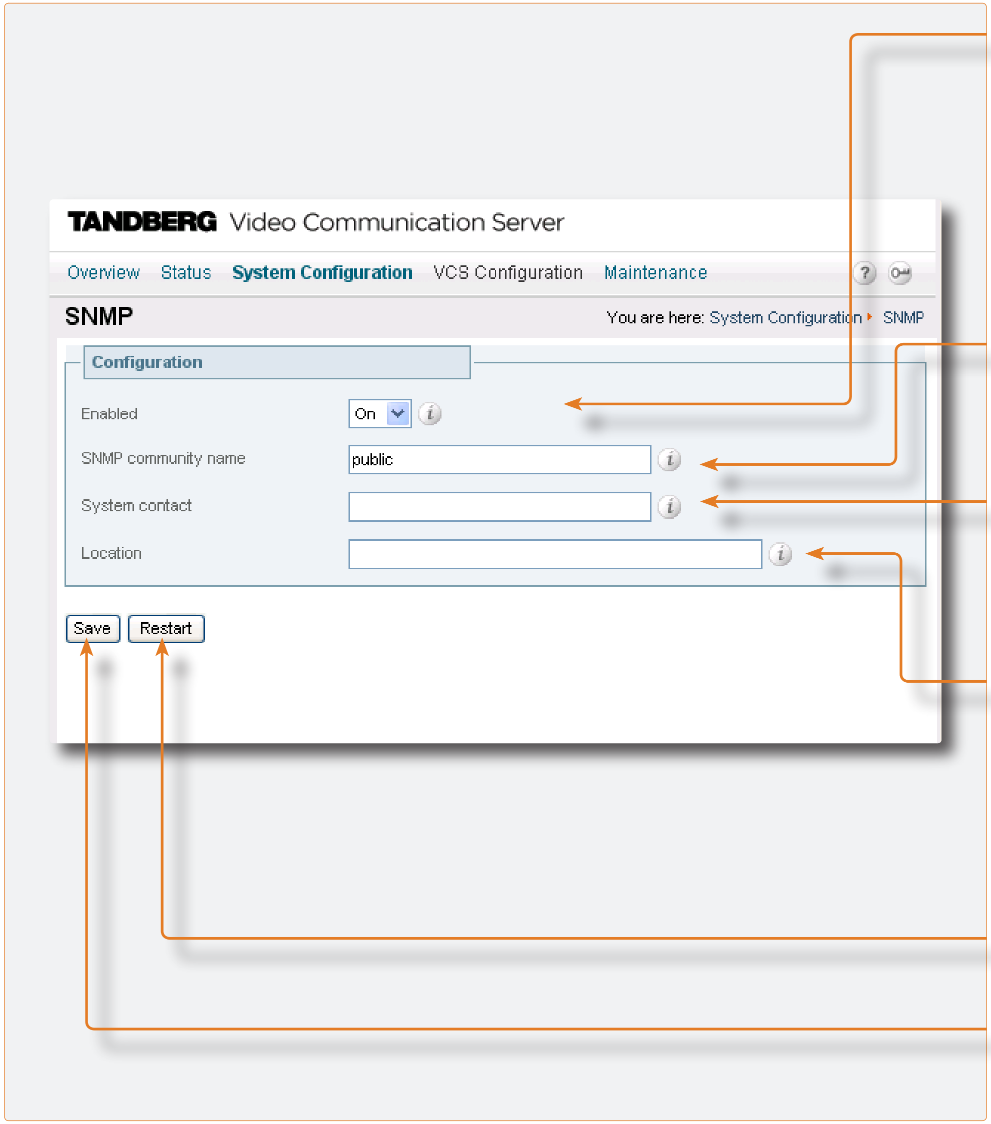
The VCS offers basic support for SNMP.

Tools such as TANDBERG Management Suite (TMS) or HP OpenView may act as SNMP network management systems (NMS). They allow you to monitor your network devices, including the VCS, for conditions that might require administrative attention.

To allow the VCS to be monitored by a SNMP NMS, you must enable SNMP on the VCS and provide the name of the SNMP community within which it resides. You may optionally provide the name of a System contact and the physical Location of the system for reference by administrators when following up on queries.

By default, SNMP is Enabled with a SNMP community name of public.

Note: the VCS does not support SNMP traps, therefore it cannot be managed via SNMP.



Enabled

Select On to enable SNMP support.

You must save your changes and restart the system for any changes to take effect.

SNMP community name

Sets the VCS's SNMP community name.

System contact

Specifies the name of the person who can be contacted regarding issues with the VCS.

Location

Specifies the physical location of the VCS.

Restart

Click here to restart the system.

Save

Click here to save your changes.

External Manager Configuration

Configuring External Manager Settings

To configure the VCS's External Manager settings:

- *System Configuration > External Manager*. You will be taken to the External Manager page.
- `xConfiguration ExternalManager`

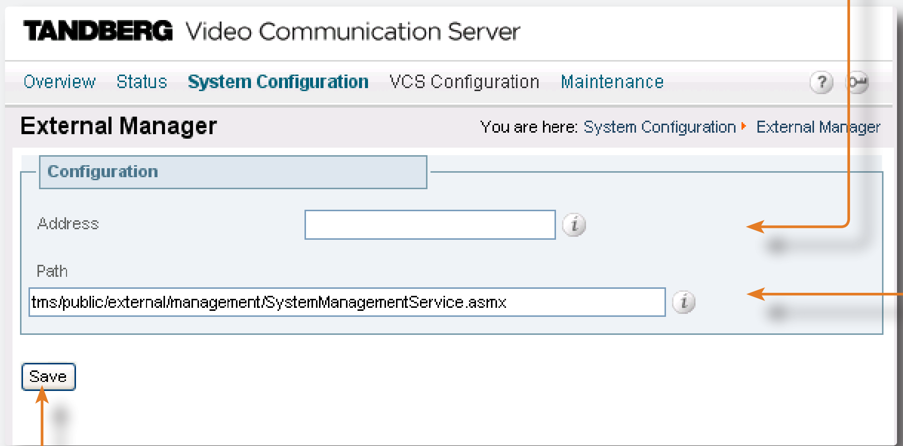
About the External Manager

An External Manager is a remote system, such as the TANDBERG Management Suite (TMS), used to monitor events occurring on the VCS, for example call attempts, connections and disconnections.

The use of an External Manager is optional.

In order to use an External Manager, you must configure the VCS with the IP address or host name and path of the External Manager to be used.

If you are using TMS as your external manager, use the default path of tms/public/ external/management/ SystemManagementService.asmx.



Address

Sets the IP address or FQDN of the External Manager.

Path

Sets the path of the External Manager.

Save

Click here to save your changes.

Backing up Configuration Settings

You are recommended to maintain a backup of your VCS configuration. To do this:

1. Use the command line interface to log on to the VCS.
2. Issue the command `xConfiguration`.
3. Save the resulting output to a file, using cut-and-paste or some other means provided by your terminal emulator.

To restore your configuration:

1. Remove the `*c` from in front of each command.
2. Paste this information back in to the command line interface.

Logging Overview

About Logging

The VCS provides a logging facility for troubleshooting and auditing purposes. The event log contains information about such things as calls, registrations, and messages sent and received.

The VCS logging facility allows you to:

- specify the amount of information that is logged by changing the event log level,
- specify an external server to which a copy of the log is written.

About Remote Logging

The event log is stored locally on the VCS. However, it is often convenient to collect copies of all event logs from various systems in a single location. A computer running a BSD-style syslog server, as defined in RFC 3164 [4] , may be used as the central log server.

A VCS will not act as a central logging server for other systems.

Enabling Remote Logging

To enable remote logging, you must configure the VCS with the address of the central log server. To do this:

- *System Configuration > Logging*.
  You will be taken to the Logging page.
- xConfiguration Log Server Address

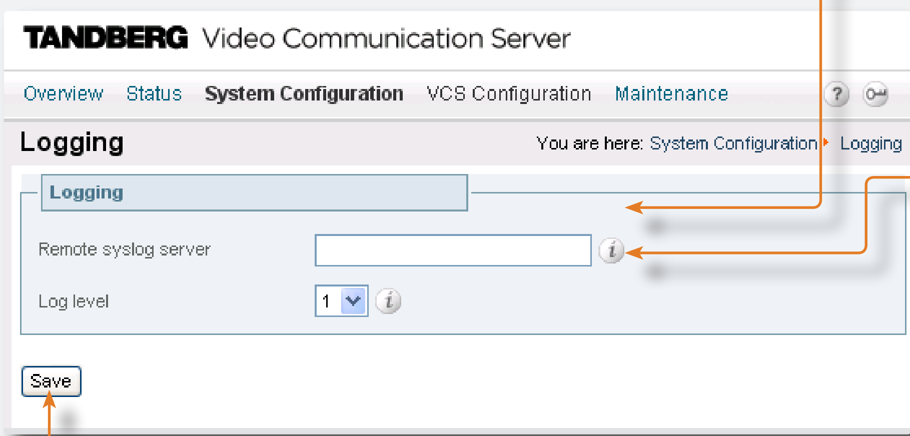
Events will be always logged locally regardless of whether or not remote logging has been enabled.

About Event Log Levels

All events have an associated level in the range 1-3, with level 1 events considered the most important. The table below gives an overview of the levels assigned to different events.

See Events Logged at Level 1, Events Logged at Level 2 and Events Logged at Level 3 for complete tables of the events logged at each level.

Level	Assigned Events
Level 1 (User)	High-level events such as registration requests and call attempts. Easily human readable. For example: • call attempt/connected/disconnected • registration attempt/accepted/rejected.
Level 2 (Protocol)	Logs of protocol messages sent and received (H.323, LDAP, etc.) excluding noisy messages such as H.460.18 keepalives and H.245 video fast-updates.
Level 3 (Protocol Verbose)	Protocol keepalives are suppressed at Level 2. At logging Level 3, keepalives are also logged.



Setting the Event Log Level

You can control which events are logged by the VCS by setting the log level. All events with a level numerically equal to and lower than the specified logging level are recorded in the event log.

To set the log level:

- *System Configuration > Logging*.
  You will be taken to the Logging page.
- xConfiguration Log Level

Remote syslog server

Enter the IP address or FQDN of the server to which the log will be written.

Log level

Select the level of logging you require.

The default is 1.

Save

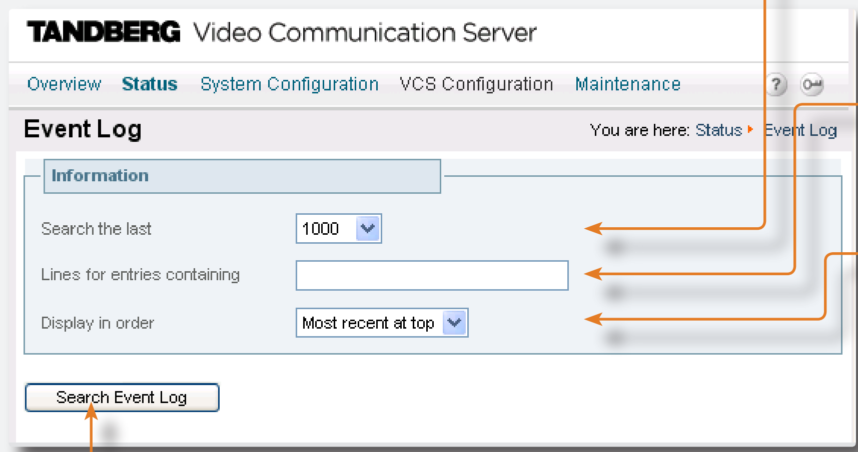
Click here to save your changes.

Event Log

Viewing the Event Log

To view the event log:

- *Status > Event Log*.
  You will be taken to the Event Log page, where you can search and view the Event Log.
- `eventlog`



Search the last

Select the number of events you wish to view or search.

Lines for entries containing

If you wish to filter your search, enter the text that you wish to search for here.

Display in order

Select whether you want the oldest or newest items to appear at the top of the log.

Search Event Log

Click here once you have configured your search options. The event log will be displayed below the Information field.

Event Log Format

The event log is displayed in an extension of the UNIX syslog format:

`date time host _ name facility _ name <PID>: message _ details`

where:

Field	Description
`date`	the local date on which the message was logged
`time`	the local time at which the message was logged
`host _ name`	the name of the system generating the log message
`facility _ name`	the name of the program generating the log message. This will be tandberg for all messages originating from TANDBERG processes, but will differ for messages from third party processes which are used in the VCS product
`message _ details`	the body of the message (see Message details field for further information)

Message Details Field

For all messages logged from the `tandberg` process the field is structured to allow easy parsing. It consists of a number of human-readable `name=value` pairs, separated by a space.

The first field is always:

Field	Example	Description
Event	`Event=RegistrationRequest`	The event which caused the log message to be generated.

and the last fields of the message are always:

Field	Example	Description
Level	`Level=1`	The level of the event being logged.
Time	`Time=2006/20/01-14:02:17`	The UTC date and time at which the event was generated.

Events Logged at Level 1

Event	Description
Eventlog Cleared	An operator cleared the event log.
Admin Session Start	An administrator has logged onto the system.
Admin Session Finish	An administrator has logged off the system.
System Configuration Changed	An item of configuration on the system has changed. The Detail event parameter contains the name of the changed configuration item and its new value.
Policy Change	A policy file has been updated.
Registration Requested	A registration has been requested.
Registration Accepted	A registration request has been accepted.
Registration Rejected	A registration request has been rejected. The Reason event parameter contains the H.225 cause code. Optionally, the Detail event parameter may contain a textual representation of the H.225 additional cause code.
Registration Removed	A registration has been removed by the VCS. The Reason event parameter specifies the reason why the registration was removed. This is one of: • Authentication change • Conflicting zones • Operator forced removal • Operator forced removal (all registrations removed)
Registration Refresh Rejected	A request to refresh a registration has been rejected.
Unregistration Requested	An unregistration request has been received.
Unregistration Rejected	An unregistration request has been rejected.
Call Answer Attempted	An attempt to answer a call has been made.
Call Attempted	A call has been attempted.
Call Connected	A call has been connected.
Call Disconnected	A call has been disconnected.
Call Rejected	A call has been rejected. The Reason event parameter contains a textual representation of the H.225 additional cause code.
Call Bandwidth Changed	The bandwidth of a call has changed.
External Server Communication Failure	Communication with an external server failed unexpectedly. The event detail data should differentiate between ‘no response’ and ‘request rejected’. Servers concerned are: • DNS • LDAP servers • Neighbor Gatekeeper • NTP servers
System Start	The operating system has started.

Events Logged at Level 1 cont...

Event	Description
System Shutdown	The operating system was shutdown.
Application Start	The VCS has started. Further detail may be provided in the event data Detail field.
Application Failed	The VCS application is out of service due to an unexpected failure.
License Limit Reached	Licensing limits for a given feature have been reached. The event detail field specifies the facility/limits concerned. Possible values for the detail field are: • Non Traversal Call Limit Reached • Traversal Call Limit Reached
Decode Error	A syntax error was encountered when decoding a SIP message.
TLS Negotiation Error	Transport Layer Security (TLS) connection failed to negotiate.

Events Logged at Level 2

Event	Description
Message Received	(H.323) An incoming message has been received.
Message Sent	(H.323) An outgoing message has been sent.
Registration Refresh Request	A request to refresh a registration has been received.
Registration Refresh Accepted	A request to refresh a registration has been accepted.
Request Received	A SIP request has been received.
Request Sent	A SIP request has been sent.
Response Received	A SIP response has been received.
Response Sent	A SIP response has been sent.

Events Logged at Level 3

Event	Description
Message Received	(SIP) An incoming message has been received.
Message Sent	(SIP) An outgoing message has been sent.

Event Data Fields

Field	Description
Protocol	Specifies which protocol was used for the communication. Valid values are: • TCP • UDP • TLS
Reason	Textual string containing any reason information associated with an event.
Service	Specifies which protocol was used for the communication. A service entry is one of: • H.323 • SIP • H.225 • H.245 • NTP • DNS • LDAP • Q.931 • Neighbor Gatekeeper
Message Type	Specifies the type of the message.
ResponseCode	SIP response code.
Src-ip	Specifies the source IP address (the IP address of the device attempting to establish communications). The source IP is recorded in the dotted decimal format: (number).(number).(number).(number) or the IPv6 colon separated format.
Dst-ip	Specifies the destination IP address (the IP address of the destination for a communication attempt). The destination IP is recorded in the same format as `Src-ip`.
Dst-port	Specifies the destination port: the IP port of the destination for a communication attempt.
Src-port	Specifies the source port: the IP port of the device attempting to establish communications.
Src-Alias	If present, the first H.323 Alias associated with the originator of the message If present, the first E.164 Alias associated with the originator of the message
Dst-Alias	If present, the first H.323 Alias associated with the recipient of the message If present, the first E.164 Alias associated with the recipient of the message
Auth	Whether call attempt has been authenticated successfully.
Method	SIP method (INVITE, BYE, UPDATE, REGISTER, SUBSCRIBE, etc)
Contact	Contact: header from REGISTER
AOR	Address of record

Event Data Fields cont...

Field	Description
`Call-Id`	The Call-ID header field uniquely identifies a particular invitation or all registrations of a particular client.
`To`	(for REGISTER requests): the AOR for the REGISTER request.
`RequestURI`	The SIP or SIPS URI indicating the user or service to which this request is being addressed.
`NumBytes`	The number of bytes sent/received in the message.
`Duration`	Request/granted registration expiry duration
`Time`	A full UTC timestamp in YYYY/MM/DD-HH:MM:SS format. Using this format permits simple ASCII text sorting/ordering to naturally sort by time. This is included due to the limitations of standard syslog timestamps.
`Level`	The level of the event as defined in section 16.3.1.

In addition to the events described above, a `syslog.info` event containing the string `MARK` will be logged once an hour to provide confirmation that logging is still active.

Working with H.323

H.323 Overview

About H.323 on the VCS

The VCS supports the H.323 protocol: it is an H.323 gatekeeper, and will provide interworking between H.323 and SIP calls. In order to support H.323, the H.323 mode must be enabled.

Using the VCS as an H.323 Gatekeeper

As an H.323 gatekeeper, the VCS accepts registrations from H.323 endpoints and provides call control functions such as address translation and admission control.

Configuring H.323 Ports

The VCS enables you to configure the listening port for H.323 registrations and call signaling, and the range of ports to be used by H.323 calls once they are established.

The default VCS configuration uses standard port numbers so you can use H.323 services out of the box without having to first set these up.

H.323 Endpoint Registration

Overview

H.323 endpoints in your network must register with the VCS in order to use it as their gatekeeper.

There are two ways an H.323 endpoint can locate a VCS with which to register: manually or automatically. The option is configured on the endpoint itself under the Gatekeeper Discovery setting (consult your endpoint manual for how to access this setting).

- If the mode is set to automatic, the endpoint will try to register with any VCS it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible VCSs will respond.
- If the mode is set to manual, the you must specify the IP address of the VCS with which you wish your endpoint to register, and the endpoint will attempt to register with that VCS only.

Registration Conflict Mode

An H.323 endpoint may attempt to register with the VCS using an alias that has already been registered on the VCS from another IP address. The reasons for this could include:

- two endpoints at different IP addresses are attempting to register using the same alias
- a single endpoint has previously registered using a particular alias. The IP address allocated to the endpoint then changes, and the endpoint is attempting to re-register using the same alias.

You can determine how the VCS will behave in this situation by configuring the Registration Conflict Mode. The options are:

- Reject: denies the registration.
- Overwrite: deletes the original registration and replaces it with the new registration.

Auto Discover

The VCS has an Auto discover setting which determines whether it will respond to the Gatekeeper Discovery Requests sent out by endpoints.

To prevent H.323 endpoints being able to register automatically with the VCS, set Auto Discover to Off. This will mean that endpoints will be able to register with the VCS only if they have been configured with the VCS's IP address.

Time to Live

H.323 endpoints must periodically re-register with the VCS in order to confirm that they are still functioning. The VCS allows you to configure the interval between these re-registrations, known as the Time to Live.

Some older endpoints do not support the ability to periodically re-register with the system. In this case, and in any other situation where the system has not had a confirmation from the endpoint within the specified period, it will send an IRQ to the endpoint to verify that it is still functioning.

Call Time to Live

Once the endpoint is in a call, the VCS will periodically poll it to confirm whether it is still in the call. The VCS allows you to configure the interval at which the endpoints are polled, known as the Call Time to Live.

The system will poll endpoints in a call regardless of whether the call type is traversal or non-traversal.

Working with H.323

Configuring H.323

H.323 settings are configured via:

- *VCS Configuration > Protocols > H.323*. You will be taken to the H.323 page.
- xConfiguration H323

H.323 Mode

Determines whether or not the VCS will provide H.323 gatekeeper functionality.

Registration UDP port

Specifies the port to be used for H.323 UDP registrations.

Call signaling TCP port

Specifies the port that listens for H.323 call signaling.

Call signaling port range start

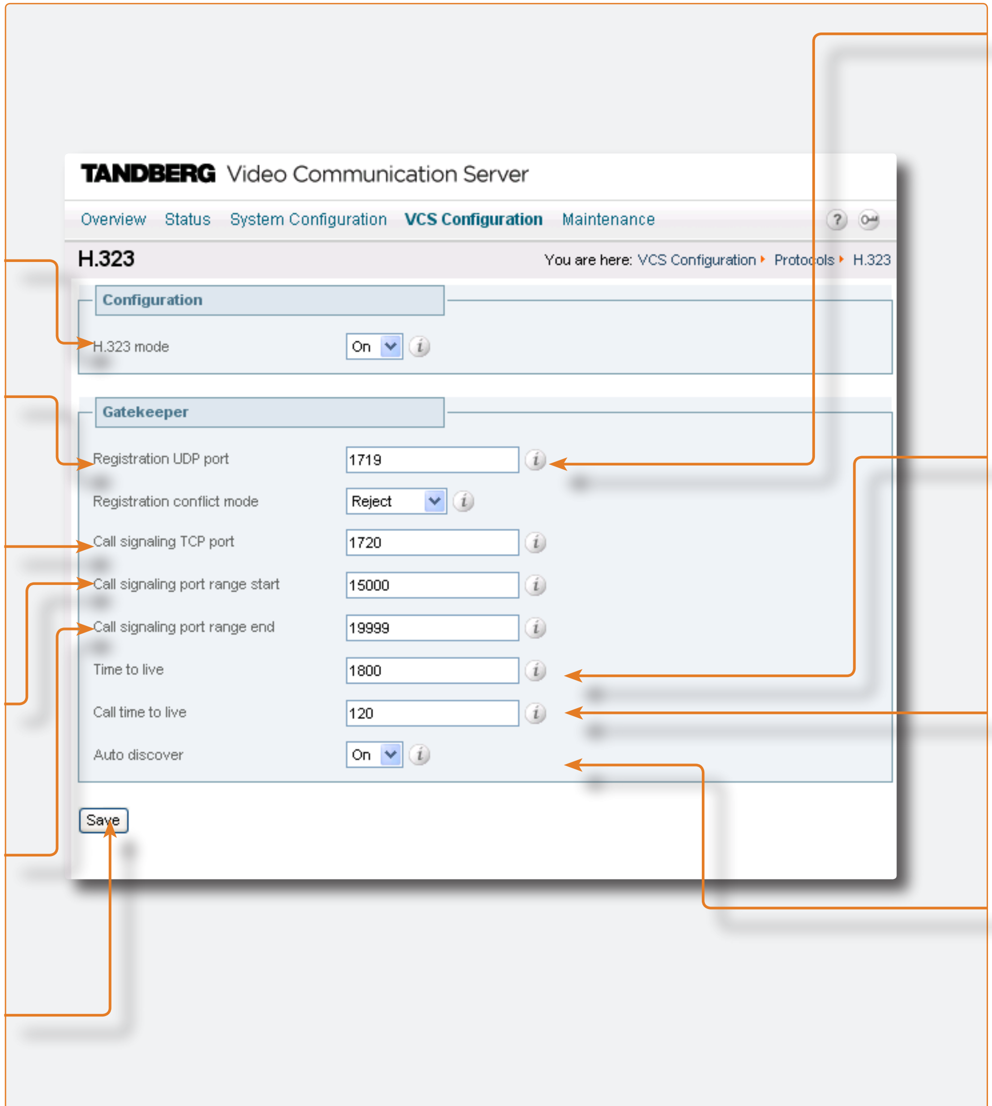
Specifies the lower port in the range to be used by H.323 calls once they are established.

Call signaling port range end

Specifies the upper port in the range to be used by H.323 calls once they are established.

Save

Click here to save your changes.



Registration conflict mode

Determines how the system will behave if an endpoint attempts to register an alias currently registered from another IP address.

Reject: denies the registration.

Overwrite: deletes the original registration and replaces it with the new registration.

Time to live

Specifies the interval (in seconds) at which an H.323 endpoint must re-register with the VCS in order to confirm that it is still functioning.

Call time to live

Specifies the interval (in seconds) at which the VCS polls the endpoints in a call to verify that they are still in the call.

Auto discover

Determines whether or not the VCS responds to gatekeeper discovery requests from endpoints.

SIP Overview

About SIP on the VCS

The VCS supports the SIP protocol: it is both a SIP Proxy and SIP Registrar, and will provide interworking between SIP and H.323 calls. In order to support SIP, SIP mode must be enabled and at least one of the SIP transport protocols must be active.

Using the VCS as a SIP Registrar

In order for a SIP endpoint to be contactable via its registered alias, it must register its location with a SIP Registrar. The VCS can act as a SIP Registrar for up to 20 domains.

SIP aliases always take the form username@domain. To enable the VCS to act as a SIP Registrar, you must configure it with the SIP Domain(s) for which it will be authoritative. It will then accept registration requests for any endpoints attempting to register with an alias that includes that domain.

If no Domains are configured, then the VCS will not act as a SIP Registrar.

Proxying Registration Requests

If the VCS has no domains configured, or it receives a registration request for a domain for which it is not acting as a Registrar, then the VCS may proxy the registration request. This depends on the SIP Registration Proxy Mode setting, as follows;

- Off: the VCS will not proxy any registration requests. The request will be rejected with a “`403 Forbidden`” message.
- Proxy to Known Only: the VCS will proxy the registration request but only to its neighbors.
- Proxy to any: the VCS will proxy the registration requests in accordance with its call policy (e.g. administrator policy and transforms). See Call Processing for more information.

This setting also impacts the VCS’s behavior when acting as a SIP Proxy Server.

Using the VCS as a SIP Proxy Server

When in SIP mode, the VCS may act as a SIP Proxy Server. The role of a Proxy Server is to forward requests (such as REGISTER and INVITE) from endpoints or other Proxy Servers. These requests are forwarded on to other Proxy Servers or to the destination endpoint.

Whether or not the VCS acts as a SIP Proxy Server, and its exact behavior when proxying requests, is determined by the SIP Registration Proxy Mode setting. This in turn depends on the presence of Route Set information in the request header and whether or not the Proxy Server from which the request was received is a Neighbor of the VCS.

A Route Set can specify the path that must be taken when requests are being proxied between an endpoint and its Registrar. For example, when a REGISTER request is proxied by a VCS, the VCS adds a Path header component to the request which signals that the VCS must be included on any call to that endpoint. The information is usually required in situations where firewalls exist and the media must follow a specified path in order to successfully traverse the firewall. For more information about the path header field, see RFC 3327 [10].

When the VCS proxies a request that contains existing Route Set information, it will forward it directly to the URI specified in the path. Any call policy configured on the VCS will therefore be bypassed. This may present a security risk if the information in the Route Set cannot be trusted. For this reason, you can configure the VCS with three different behaviors when proxying requests, as follows:

- If the SIP Registration Proxy Mode setting is Off, the VCS will not proxy any requests that have an existing Route Set. Requests that do not have an existing Route Set will still be proxied in accordance with existing call policy (e.g. zone searches and transforms). This setting provides the highest level of security.
- If the setting is Proxy to Known Only, the VCS will proxy requests with an existing Route Set only if the request was received from a Neighbor zone (including Traversal Client and Traversal Server zones). Requests that do not have an existing Route Set will be proxied in accordance with existing call policy.
- If the setting is Proxy to any, the VCS will proxy all requests. Those with existing Route Sets will be proxied to the specified URI; those without will be proxied in accordance with existing call policy.

SIP Registration Expiry

SIP endpoints must periodically re-register with the SIP Registrar in order to prevent their registration expiring. You can determine the interval with which SIP endpoints must register with the VCS.

This setting applies only when the VCS is acting as a SIP Registrar, and to endpoints registered with the VCS. It does not apply to endpoints whose registrations are being proxied through the VCS.

SIP protocols and ports

The VCS supports SIP over UDP, TCP and TLS transport protocols. You can configure whether or not incoming calls using each protocol are supported, and if so, the ports on which the VCS will listen for such calls.

At least one of these protocols must be set to a Mode of On in order for SIP functionality to be supported.

Working with SIP

Configuring SIP - Registrations, Protocols and Ports

SIP settings are configured via:

- *VCS Configuration > Protocols > SIP > Configuration*.
  You will be taken to the SIP page.
- `xConfiguration SIP`

SIP mode

Determines whether or not the VCS will provide SIP functionality (i.e. SIP Registrar and SIP proxy services).

Registration expire delta

Specifies the period within which a SIP endpoint must re-register to prevent its registration expiring.

SIP registration proxy mode

Specifies how proxied registrations and invites will be handled.

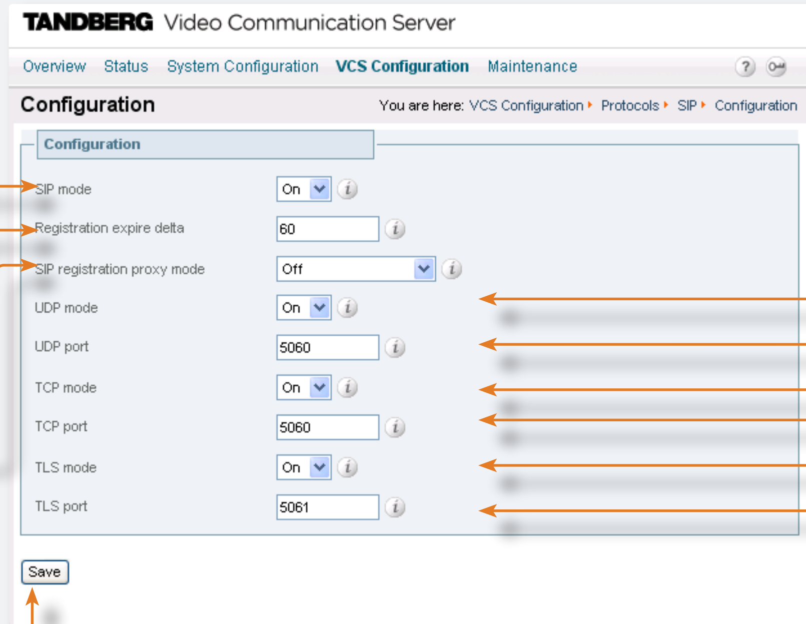
Off: Registration requests will not be proxied (but will still be permitted locally if the VCS is authoritative for that domain). Invite requests with existing Route Sets will be rejected.

Proxy to known only: Registration requests will be proxied, and invite requests will be proxied only if the Route Set contains the URI(s) of Neighbors

Proxy to any: Registration requests and invite requests will always be proxied.

Save

Click here to save your changes.



UDP mode

Determines whether or not incoming SIP calls using the UDP protocol will be allowed.

The default is On.

UDP port

Specifies the listening port for incoming SIP calls over UDP.

The default is 5060.

TCP mode

Determines whether or not incoming SIP calls using the TCP protocol will be allowed.

The default is On.

TCP port

Specifies the listening port for incoming SIP calls over TCP.

The default is 5060.

TLS mode

Determines whether or not incoming SIP calls using the TLS protocol will be allowed.

The default is On.

TLS port

Specifies the listening port for incoming SIP calls over TLS.

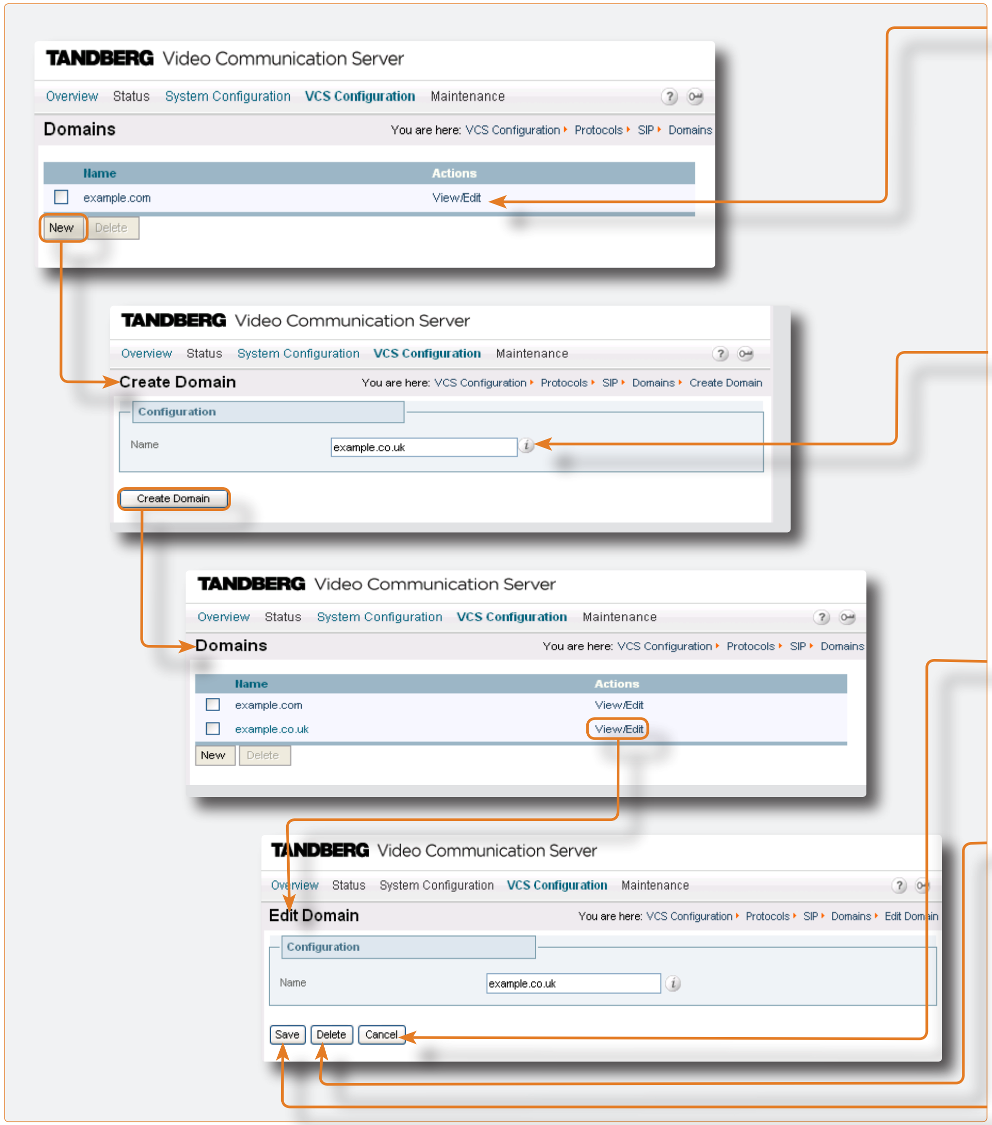
The default is 5061.

Working with SIP

Configuring SIP - Domains

SIP domains are configured via:

- *VCS Configuration > Protocols >SIP > Domains*.
  You will be taken to the Domains page.
  - To add a new domain, click New.
    You will be taken to the Create Domain page.
    Enter the domain in the Name field and click Create Domain.
    The new domain will be added and you will be returned to the Domains page.
  - To edit the name of an existing domain, click View/Edit.
    You will be taken to the Edit Domain page.
    Edit the Name of the domain and click Save.
    The name of the domain will be changed.
  - To delete an existing domain, click View/Edit.
    You will be taken to the Edit Domain page.
    Click Delete.
    The domain will be deleted and you will be returned to the Domains page.
- [xCommand DomainAdd]
- [xConfiguration SIP Domains]



View/Edit

Click here to change the domain name or delete the domain.

Name

Specifies a domain for which the VCS is authoritative.

The VCS will act as a SIP Registrar for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain.

Cancel

Click here to return to the Domains page without saving your changes.

Delete

Click here to delete the domain and return to the Domains page.

Save

Click here to save your changes.

Overview

About Interworking

The VCS is able to act as a gateway between SIP and H.323, translating calls from one protocol to the other. This is known as “interworking”.

By default, the VCS will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.

You can add an additional option key that will allow the VCS to act as SIP-H.323 gateway regardless of whether the endpoints are locally registered. Contact your TANDBERG representative for further information.

In either case, you also always have the option to disable interworking.

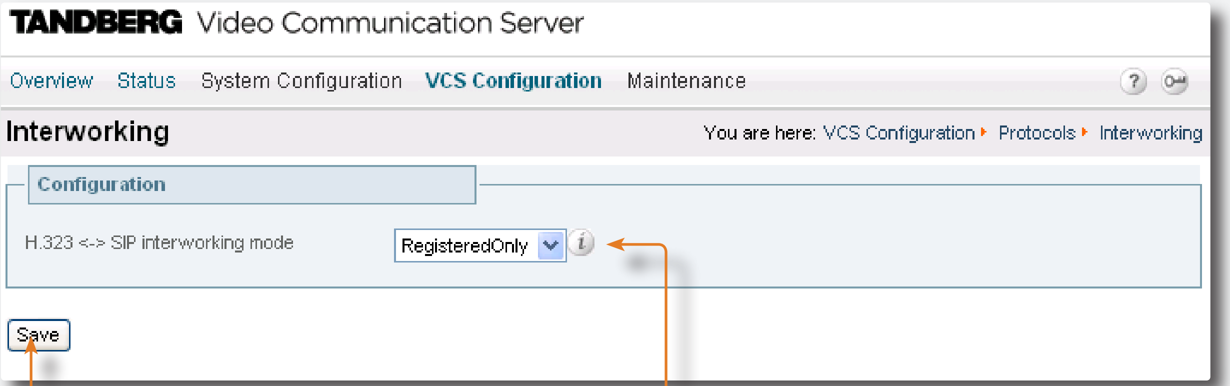
An interworking call is a traversal call, and will therefore consume one traversal licence for the duration of the call.

A call between two H.323 endpoints each registered to a different VCS may be routed in such a way that it is interworked from H.323 to SIP and back to H.323. (For example, if the two VCSs are only able to connect via SIP.) In this case, the two H.323 endpoints involved must support H.263 video. If they do not (for example, if H.263 has been disabled) the call will still be established but it will be audio only.

Configuring Interworking

Interworking is enabled via:

- *VCS Configuration > Protocols > Interworking*. You will be taken to the Interworking page.
- xConfiguration Interworking Mode



Save

Click here to save your changes.

H.323 <-> SIP interworking mode

Determines whether or not the VCS will act as a gateway between SIP and H.323 calls.

Off: the VCS will not act as a SIP-H.323 gateway.

RegisteredOnly: the VCS will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.

On: the VCS will act as SIP-H.323 gateway regardless of whether the endpoints are locally registered. You must have the appropriate option key enabled to use this feature.

Registration Control

Registration Overview

Endpoint Registration

In order for an endpoint to use the TANDBERG VCS, the endpoint must first register with the VCS. The VCS can be configured to control which devices are allowed to register with it. Two separate mechanisms are provided:

- an authentication process based on the username and password supplied by the endpoint
- a simple Registration Restriction Policy that uses Allow Lists or Deny Lists to specify which aliases can and cannot register with the VCS.

It is possible to use both mechanisms together. For example, you can use authentication to verify an endpoint's identity from a corporate directory, and registration restriction to control which of those authenticated endpoints may register with a particular VCS.

This section gives an overview of how endpoints and other devices register with the VCS, and then describes the two mechanisms by which registrations can be restricted.

Registrations on a VCS Border Controller

If a traversal-enabled endpoint registers directly with a VCS Border Controller, the VCS Border Controller will provide VCS services to that endpoint in addition to firewall traversal. Traversal-enabled endpoints include all TANDBERG Expressway™ endpoints and third party endpoints which support the ITU H.460.18 and H.460.19 standards.

Endpoints that are not traversal-enabled can still register with a VCS Border Controller, but they may not be able to make and/or receive calls through the firewall successfully. This will depend on a number of factors:

- whether the endpoint is using SIP or H.323
- the endpoint's position in relation to the firewall
- whether there is a NAT in use
- whether the endpoint is using a public IP address

For example, if an endpoint is behind a NAT and/or firewall. it may not be able to receive incoming calls and may not be able to receive media for calls they have initiated.

MCU, Gateway and Content Server Registration

H.323 systems such as gateways, MCUs and Content Servers can also register with a VCS. They are known as locally registered services. These systems are configured with their own prefix, which they provide to the VCS when registering. The VCS will then know to route all calls that begin with that prefix to the gateway, MCU or Content Server as appropriate. These prefixes can also be used to control registrations.

SIP devices cannot register prefixes. If your dial plan dictates that a SIP device should be reached via a particular prefix, then you should add the device as a neighbor zone with a pattern match equal to the prefix to be used.

Registration Overview

Finding a VCS with which to Register

Before an endpoint can register with a VCS, it must determine which VCS it can or should be registering with. This setting is configured on the endpoint, and the process is different for SIP and H.323.

SIP

SIP endpoints must find a SIP Registrar with which to register. The SIP Registrar maintains a record of the endpoint's details against the endpoint's Address of Record (AOR). When a call is received for that AOR, the SIP Registrar refers to the record in order to find the endpoint to which it corresponds. (Note that the same AOR can be used by more than one SIP endpoint at the same time.)

The SIP Registrar will only accept registrations for domains for which it is authoritative.

There are two ways a SIP endpoint can locate a Registrar with which to register: manually or automatically. The option is configured on the endpoint itself under the SIP Server Discovery option (consult your endpoint user guide for how to access this setting).

- If the mode is set to automatic, the endpoint will send a REGISTER message to its SIP Server. This will be forwarded (via DNS if necessary) to the Registrar that is authoritative for the domain with which the endpoint is attempting to register. For example, if an endpoint is attempting to register with a URI of john.smith@example.com, the request will be sent to the Registrar authoritative for the domain example.com.
- If the mode is set to manual, the user must specify the IP address of the Registrar with which they wish to register, and the endpoint will attempt to register with that Registrar only.

The VCS is a SIP Server for endpoints in its local zone, and can also act as a SIP Registrar.

- If the VCS is acting as the endpoint's SIP Server and SIP Registrar, when the registration request is received from the endpoint it will be accepted by the VCS and the endpoint will be registered and able to receive inbound calls. See Using the VCS as a SIP Registrar for more information.
- If the VCS is acting as the endpoint's SIP server but is not a SIP Registrar, it will proxy the registration request. See Proxying registration requests for more information.

H.323

There are two ways an H.323 endpoint can locate a VCS with which to register: manually or automatically. The option is configured on the endpoint itself under the Gatekeeper Discovery setting (consult your endpoint manual for how to access this setting).

- If the mode is set to automatic, the endpoint will try to register with any VCS it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible VCSs will respond.
- If the mode is set to manual, you must specify the IP address of the VCS with which you wish your endpoint to register, and the endpoint will attempt to register with that VCS only.

Preventing automatic registrations

You can prevent H.323 endpoints being able to register automatically with the VCS by disabling Auto Discovery on the VCS. The Auto Discovery setting determines whether the VCS responds to the Gatekeeper Discovery requests sent out by endpoints.

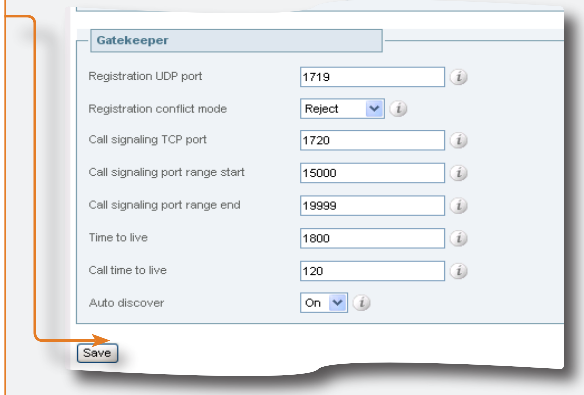
To configure the Auto Discovery setting:

- *VCS Configuration > Protocols > H.323*.
  You will be taken to the H.323 page.
- `H323 Gatekeeper AutoDiscovery`

Auto discover

On: The VCS will respond to Gatekeeper discovery requests.

Off: The VCS will not respond to Gatekeeper discovery requests. H.323 endpoints will be able to register with the VCS only if their Gatekeeper Discovery setting is Manual and they have entered the IP address of the VCS.



Authentication

About Authentication

The VCS can be configured to use a username and password-based challenge-response scheme to permit endpoint registrations. This process is known as authentication.

In order to authenticate with the VCS, the endpoint must supply it with a username. For TANDBERG endpoints using H.323, the username is the endpoint's Authentication ID; for TANDBERG endpoints using SIP it is the endpoint's Authentication Username.

For details of how to configure endpoints with a username and password, please consult the endpoint manual.

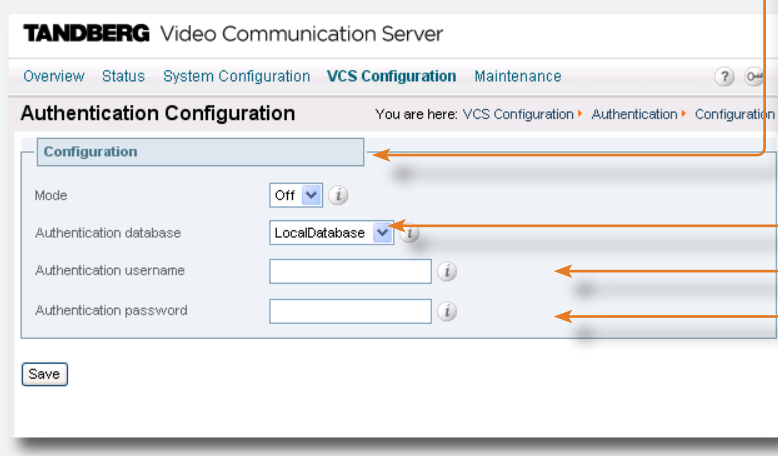
In order to verify the identity of the device, the VCS needs access to a database on which all authentication credential information (usernames, passwords, and other relevant information) is stored. This database may be located either locally on the VCS, or on an LDAP Directory Server. The VCS looks up the endpoint's username in the database and retrieves the authentication credentials for that entry. If the credentials match those supplied by the endpoint, the registration is allowed to proceed.

The VCS supports the ITU H.235 specification [1] for authenticating the identity of H.323 network devices with which it communicates.

Configuring Authentication

To configure Authentication options:

- *VCS Configuration > Authentication > Configuration*
  You will be taken to the Authentication Configuration page (shown below).
- `xConfiguration Authentication`



Mode

On: all endpoints must authenticate with the VCS before registering.

Off: no authentication is required for endpoints.

The default is Off.

Authentication database

Determines which database the VCS will use during authentication.

LocalDatabase: the local database is used. You must configure the Local database to use this option.

LDAP: A remote LDAP database is used. You must configure the LDAP server to use this option.

The default is LocalDatabase.

Authentication password

Specifies the password to be used by the VCS (in conjunction with the Authentication username) when the VCS is authenticating with another system.

Authentication username

The Authentication Username is the name that the VCS uses when authenticating with other systems. For example, when forwarding an invite from an endpoint to another VCS, that other system may have authentication enabled and will therefore require your local VCS to provide it with a username and password. Traversal clients must always successfully authenticate with traversal servers before they can be used.

The authentication username and password for your local VCS must be stored on either the local database or LDAP database (depending on which has been enabled), along with all the other authentication usernames and passwords. When your local VCS receives an authentication request, it looks up its own username in the database and sends the corresponding authentication credentials, along with the username, to the system that requested it. If the username and authentication credentials match those stored on the requesting system's database, the communication can continue.

Authentication

Authentication using an LDAP Server

If the VCS is using an LDAP server for authentication, the process is as follows:

1. The endpoint presents its username and authentication credentials (these are generated using its password) to the VCS, and the alias(es) with which it wishes to register
2. The VCS looks up the username in the LDAP database and obtains the authentication and alias information for that entry.
3. If the authentication credentials match those supplied by the endpoint, the registration will continue.

The VCS will then determine which alias(es) the endpoint will be allowed to attempt to register with, based on the alias origin setting. For H.323 endpoints, you can use this setting to override the aliases presented by the endpoint with those in the H.350 directory, or you can use them in addition to the endpoint's aliases. For SIP endpoints, you can use this setting to reject a registration if the endpoint's AOR does not match that in the LDAP database.

Configuring the LDAP Server Directory

The directory on the LDAP server should be configured to implement the ITU H.350 specification [2] to store credentials for devices with which the VCS communicates. The directory should also be configured with the aliases of endpoints that will register with the VCS.

For instructions on how to configure common LDAP servers, see the Appendix LDAP Configuration.

Securing the LDAP Connection with TLS

The traffic between the VCS and the LDAP server can be encrypted using Transport Layer Security (TLS).

To use TLS:

- LDAP encryption must be set to TLS
- the LDAP server must have a valid certificate installed, verifying its identity
- The VCS must trust the certificate installed on the LDAP server.

TLS can be difficult to configure, so we recommend that you confirm that your LDAP database is working correctly before you attempt to secure the connection with TLS. We also recommend that you use a third party LDAP browser to verify that your LDAP server is correctly configured to use TLS.

For information on how to configure the VCS to trust the certificate installed on the LDAP server, see About security.

Alias Origin Setting

This setting determines the alias(es) with which the endpoint will attempt to register.

LDAP

The alias(es) presented by the endpoint will be used as long as they are listed in the LDAP database for the endpoint's username.

- If an endpoint presents an alias that is listed in the LDAP database, it will be registered with that alias.
- If more than one alias is listed in the LDAP database for that username, the endpoint will be registered with only those aliases that it has presented.
- If an endpoint presents an alias that is not in the LDAP database, it will not be registered with that alias.
- If an endpoint presents more than one alias but none are listed in the LDAP database, it will not be allowed to register.
- If no aliases are presented by the endpoint, it will be registered with all the aliases listed in the LDAP database for its username. (This is to allow for MCUs which additively register aliases for conferences, for example the TANDBERG MPS (J4.0 and later) which registers ad-hoc conferences.)
- If no aliases are listed in the LDAP database for the endpoint's username, then the endpoint will be registered with all the aliases it presented.

Combined

The alias(es) presented by the endpoint will be used in addition to any that are listed in the LDAP database for the endpoint's username. In other words, this is the same as for LDAP, with one exception:

- If an endpoint presents an alias that is not in the LDAP database, it will be allowed to register with that alias.

Endpoint

The alias(es) presented by the endpoint will be used; any in the LDAP database will be ignored.

- If no aliases are presented by the endpoint, it will not be allowed to register.

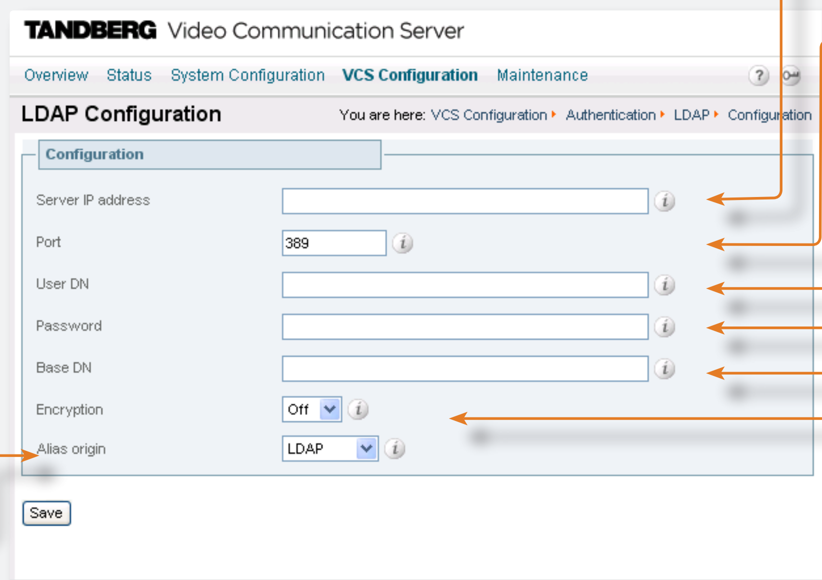
Registration Control

Authentication

Configuring LDAP Server settings

To configure the settings for accessing the LDAP server:

- *VCS Configuration > Authentication > LDAP > Configuration.*
  You will be taken to the LDAP Configuration page.
- xConfiguration LDAP
- xConfiguration Authentication LDAP



Server IP address

The IP address or FQDN of the LDAP server.

Port

The IP port of the LDAP server.

UserDN

The user distinguished name to be used by the VCS when binding to the LDAP server.

Password

The password to be used by the VCS when binding to the LDAP server.

Base DN

The area of the directory on the LDAP server to be searched for the credential information.

This should be specified as the Distinguished Name (DN) in the LDAP directory under which the H.350 objects reside.

Encryption

Determines whether the connection to the LDAP server will be encrypted. (For more information on configuring encryption, see Securing the LDAP connection with TLS.)

TLS: TLS Encryption will be used for the connection with the LDAP server.

Off: No encryption will be used.

The default is Off.

Alias origin

Determines the source of the alias(es) with which the endpoint will be registered.

LDAP: The aliases listed in the LDAP database for the endpoint's username will be used; those presented by the endpoint will be ignored.

Endpoint: The aliases presented by the endpoint will be used; any in the LDAP database will be ignored.

Combined: The endpoint will be registered both with the aliases which it has presented and with those configured in the LDAP database.

The default is LDAP.

Authentication

Authentication using a Local Database

The local database is included as part of your VCS system. It consists of a list of usernames and passwords, which you add via the web interface and/or the CLI. The database can hold up to 2500 entries.

Configuring the Local Database

To manage entries in the Local Database:

- *VCS Configuration > Authentication > Local Database.*
  You will be taken to the Credentials page.
- xConfiguration Authentication Credential
- xCommand CredentialAdd
- xCommand CredentialDelete

New

Select New to add a new entry to the Local Database. You will be taken to the Create Credential page.

Name

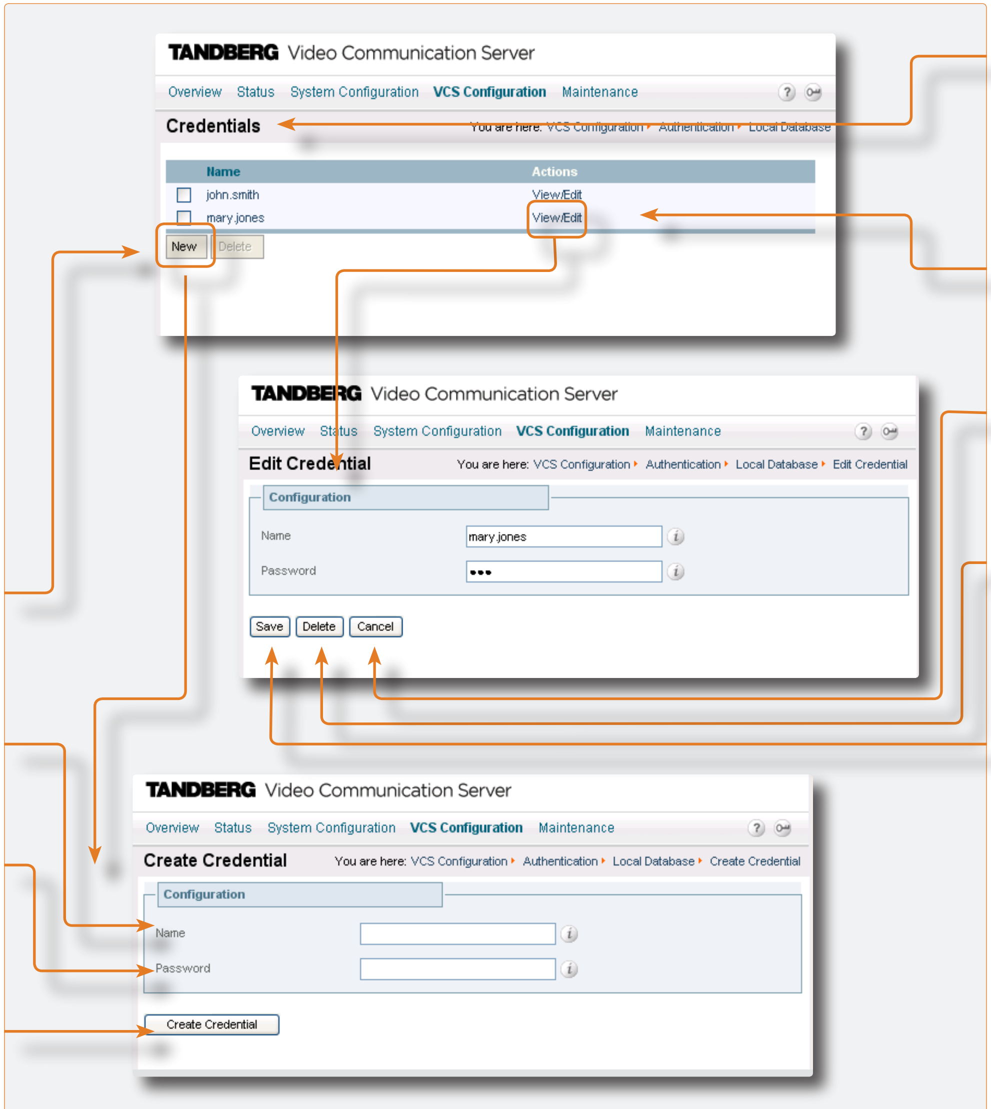
The username used by the endpoint when authenticating with the VCS.

Password

The password used by the endpoint when authenticating with the VCS.

Create Credential

Select Create Credential to add the new entry to the Local Database and return to the Credentials page.



Credentials

The Credentials page shows all the existing entries in the Local Database.

You can sort these entries by clicking on the Name column heading.

View/Edit

Select View/Edit to add a make changes to an existing entry. You will be taken to the Edit Credential page.

Cancel

Returns you to the Credentials page without saving your changes.

Delete

Removes the entry from the Local Database and returns you to the Credentials page.

Save

Saves the changes you have made.

The same credentials can be used by more than one endpoint - you do not need to have a separate entry in the database for each endpoint.

Registration Control

Registering Aliases

About Alias Registration

Once the authentication process (if required) has been completed, the endpoint will then attempt to register its alias(es) with the VCS.

H.323 Alias Registration

When registering, the H.323 endpoint presents the VCS with one or more of the following:

- one or more H.323 IDs
- one or more E.164 aliases
- one or more URIs.

Users of other registered endpoints can then call the endpoint by dialing any of these aliases.

We recommended that you register your H.323 endpoints using a URI. This facilitates interworking between SIP and H.323, as SIP endpoints register using a URI as standard.

We recommended that you do not use aliases that reveal sensitive information. Due to the nature of H.323, call setup information is exchanged in an unencrypted form.

SIP Alias Registration

When registering, the SIP endpoint presents the VCS with its contact address (IP address) and logical address (Address of Record). The logical address is considered to be its alias, and will generally be in the form of a URI.

Attempts to Register using an Existing Alias

An endpoint may attempt to register with the VCS using an alias that is already registered to the system. How this is managed depends on how the VCS is configured and whether the endpoint is SIP or H.323.

SIP

A SIP endpoint will always be allowed to register using an alias that is already in use from another IP address. When a call is received for this alias, all endpoints registered using that alias will be called simultaneously. This SIP feature is known as "forking".

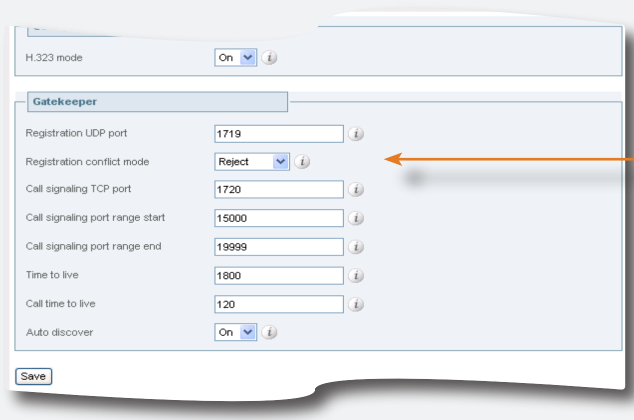
H.323

An H.323 endpoint may attempt to register with the VCS using an alias that has already been registered on the VCS from another IP address. The reasons for this could include:

- two endpoints at different IP addresses are attempting to register using the same alias
- a single endpoint has previously registered using a particular alias. The IP address allocated to the endpoint then changes, and the endpoint is attempting to re-register using the same alias.

You can determine how the VCS will behave in this situation by configuring the Registration Conflict Mode. This is done via:

- *VCS Configuration > Protocols > H.323*. You will be taken to the H.323 page.
- `xConfiguration H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite>`



Registration conflict mode

Determines what will happen when an H.323 endpoint attempts to register using an alias that has already been registered from another IP address.

Reject: The registration from the new IP address will be rejected. This is useful if your priority is to prevent two users registering with the same alias.

Overwrite: The existing registration will be overwritten using the new IP address. This is useful if your network is such that endpoints are often allocated new IP addresses, because it will prevent unwanted registration rejections.

The default is Reject.

Registration Control

Allow and Deny Lists

About Allow and Deny Lists

When an endpoint attempts to register with the VCS it presents a list of aliases. You can control which endpoints are allowed to register by setting the Restriction Policy to AllowList or DenyList and then including any one of the endpoint's aliases on the Allow List or the Deny list as appropriate. Each list can contain up to 2,500 entries. When an endpoint attempts to register, each of its aliases is compared with the patterns in the relevant list to see if it matches. Only one of the aliases needs to appear in the Allow List or the Deny List for the registration to be allowed or denied.

For example, If the Registration Restriction policy is set to DenyList and an endpoint attempts to register using three aliases, one of which matches a pattern on the Deny list, that endpoint's registration will be denied. Likewise, if the Registration Restriction policy is set to AllowList, only one of the endpoint's aliases needs to match a pattern on the Allow list for it to be allowed to register using all its aliases.

Patterns and Pattern Types

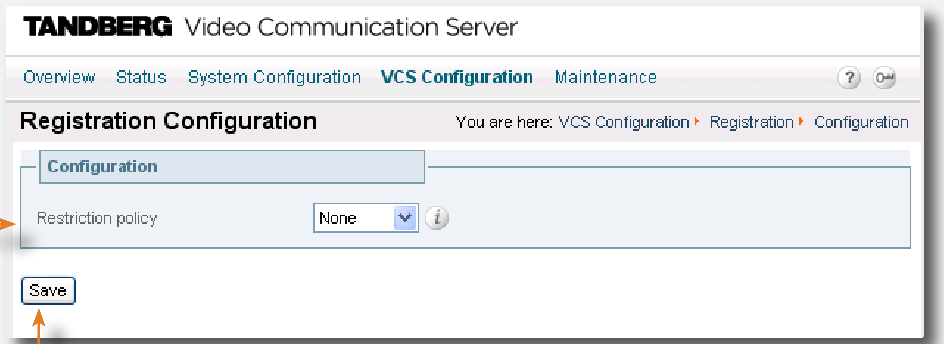
Entries on the Allow List and Deny List are a combination of Pattern and Type. The Pattern specifies the string to be matched; the Type determines whether that string;

- must match the Pattern exactly (Exact)
- must appear at the start of the alias (Prefix)
- must appear at the end of the alias (Suffix)
- is in the form of a Regular Expression (Regex).

Activating use of Allow or Deny Lists

To activate the use of Allow or Deny lists to determine which aliases are allowed to register with the VCS:

- *VCS Configuration > Registration > Configuration*.
  You will be taken to the Registration Configuration page.
- `xConfiguration Registration RestrictionPolicy`



Restriction policy

Specifies the policy to be used when determining which endpoints may register with the VCS.

None: Any endpoint may register.

AllowList: Only those endpoints with an alias that matches an entry in the Allow List may register.

DenyList: All endpoints may register, unless they match an entry on the Deny List.

The default is None.

Save

Click here to save your changes.

Allow Lists and Deny Lists are mutually exclusive: only one may be in use at any given time.

Registration Control

Allow and Deny lists

Managing Entries in the Allow List

To view and manage the entries in the Allow List:

- *VCS Configuration > Registration > Allow List*.
  You will be taken to the Registration Allow List page.
- xCommand AllowListAdd
- xConfiguration Registration AllowList

New

Click here to add a new entry to the Allow List. You will be taken to the Create Allow Pattern page.

Pattern

Enter the pattern you wish to add to the Allow List.

Type

Select the way in which the Pattern must match the alias for the registration to be allowed. Options are:

Exact: the alias must match the Pattern exactly.

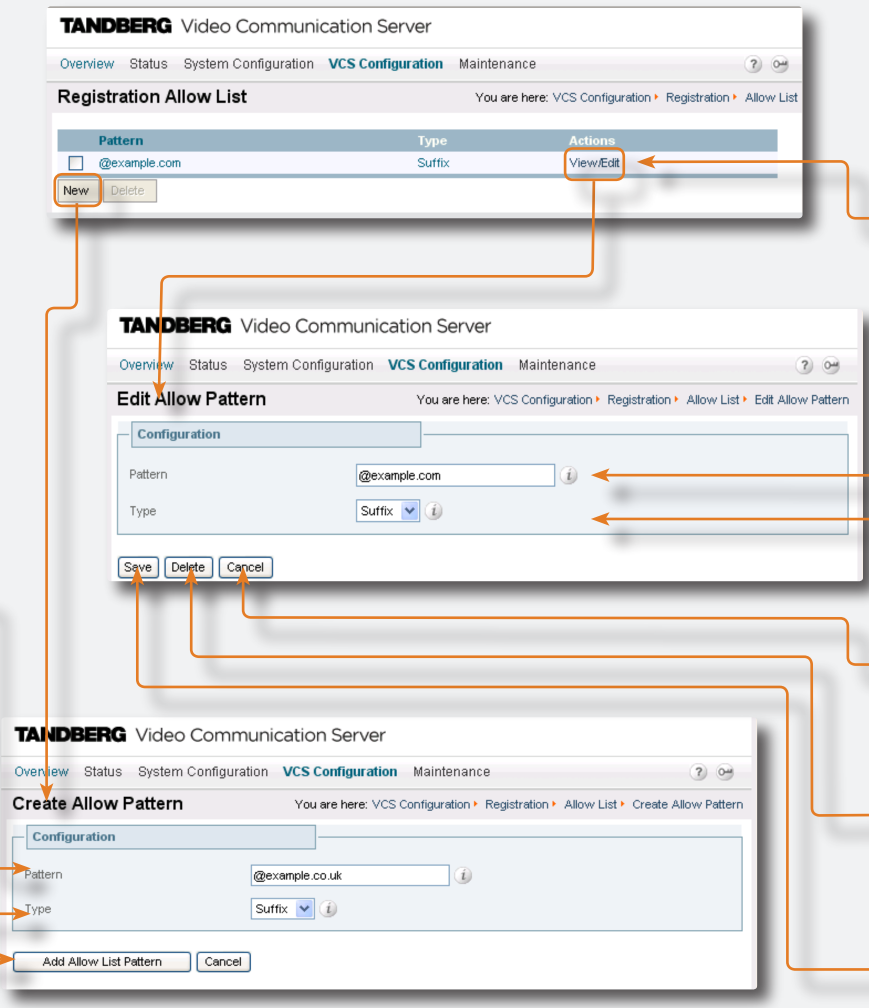
Prefix: the alias must begin with the Pattern.

Suffix: the alias must end with the Pattern.

Regex: the Pattern is a regular expression. See Regular Expression Reference for further information.

Add Allow List Pattern

Click here to save the entry and return to the Registration Allow List page.



Registration Allow List

This page shows all the existing entries in the Allow List.

You can sort these entries by clicking on the relevant column heading.

View/Edit

Select View/Edit to make changes to an existing entry. You will be taken to the Edit Allow Pattern page.

Pattern

Edit the pattern.

Type

Edit the type.

Cancel

Select Cancel to return to the Registration Allow List page without saving your changes.

Delete

Select Delete to remove the registration from the list.

Save

Select Save to save your changes.

Allow and Deny lists

Managing Entries in the Deny List

To view and manage the entries in the Deny List:

- *VCS Configuration > Registration > Deny List*.
  You will be taken to the Registration Deny List page.
- xCommand DenyListAdd
- xConfiguration Registration DenyList

New

Click here to add a new entry to the Deny List. You will be taken to the Create Deny Pattern page.

Pattern

Enter the pattern you wish to add to the Deny List.

Type

Select the way in which the Pattern must match the alias for the registration to be denied. Options are:

Exact: the alias must match the Pattern exactly.

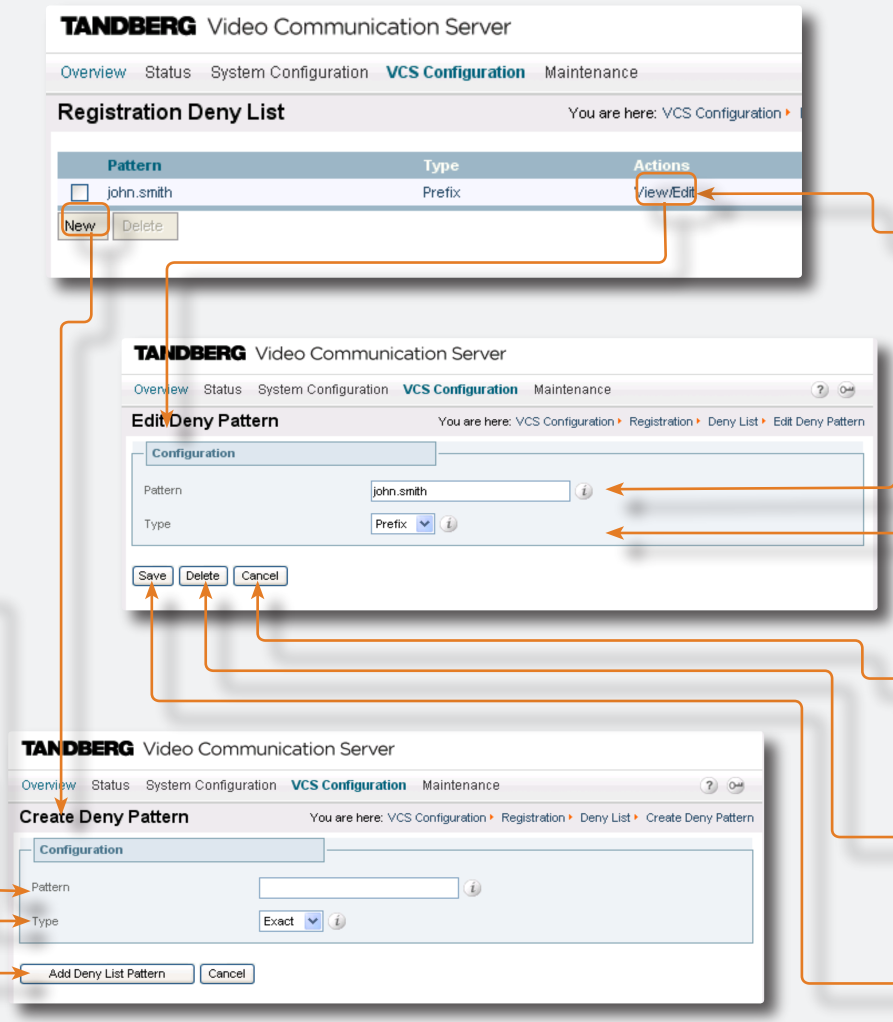
Prefix: the alias must begin with the Pattern.

Suffix: the alias must end with the Pattern.

Regex: the Pattern is a regular expression. See Regular Expression Reference for further information.

Add Deny List Pattern

Click here to save the entry and return to the Registration Deny List page.



Registration Deny List

This page shows all the existing entries in the Deny List.

You can sort these entries by clicking on the relevant column heading.

View/Edit

Select View/Edit to make changes to an existing entry. You will be taken to the Edit Deny Pattern page.

Pattern

Edit the pattern.

Type

Edit the type.

Cancel

Select Cancel to return to the Registration Deny List page without saving your changes.

Delete

Select Delete to remove the registration from the list.

Save

Select Save to save your changes.

Overview

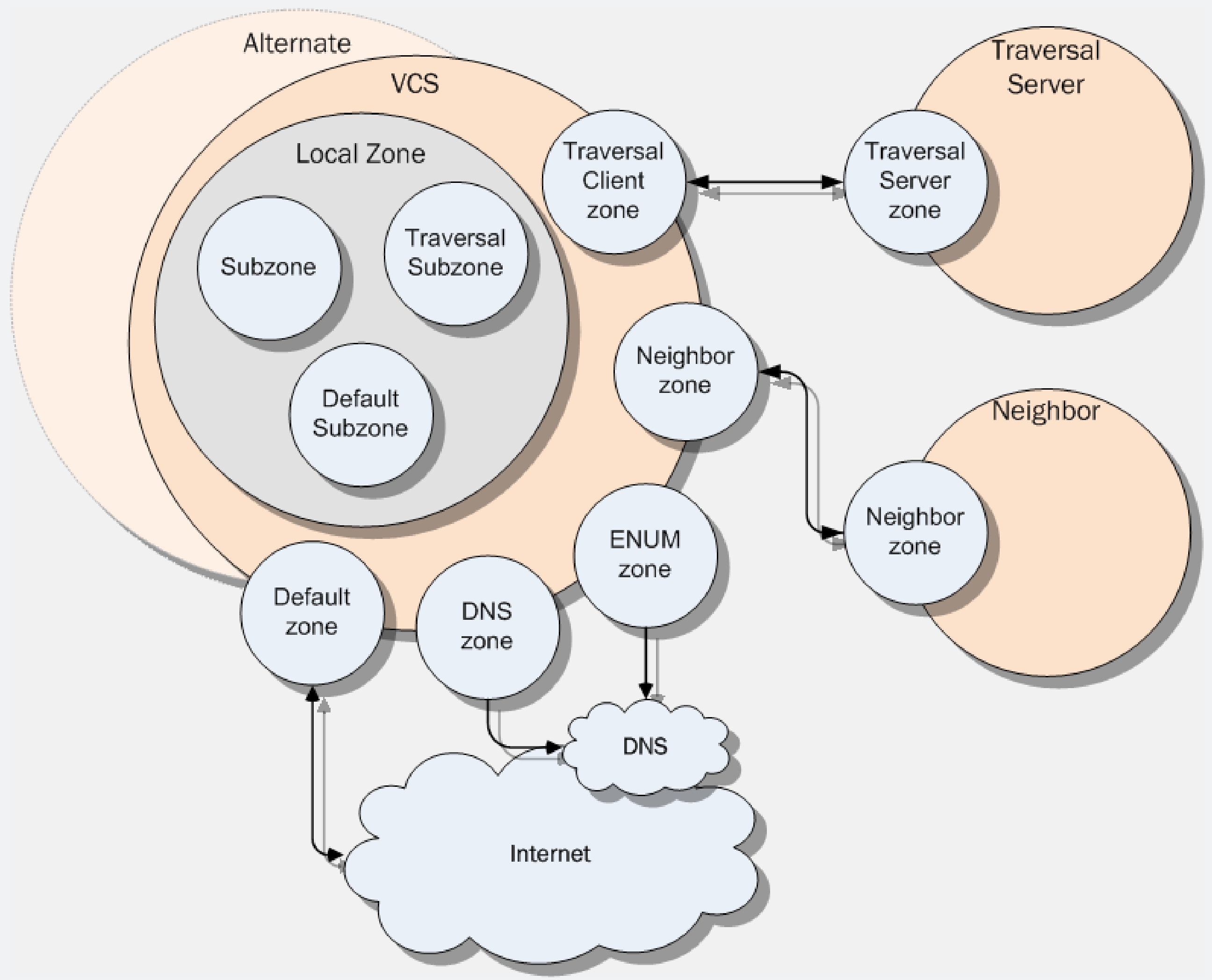
About your Video Communications Network

The most basic implementation of a TANDBERG video communications network is a single VCS connected to the internet with one or more endpoints registered to it. However, depending on the size and complexity of your enterprise the VCS may be part of a network of endpoints, other VCSs and other network infrastructure devices, with one or more firewalls between it and the internet. In addition, you may wish to apply restrictions to the amount of bandwidth used by and between different parts of your network.

This section will give you an overview of the different parts of the video communications network and the ways in which they can be connected. This information should allow you to configure your VCS to best suit your own infrastructure.

Example

The diagram opposite shows how the different components of the network fit together. These components are described in more detail in the sections that follow.



Local Zone and Subzones

About the Local Zone and its Subzones

The collection of all endpoints, gateways, MCUs and Content Servers registered with the VCS make up its Local Zone.

The Local Zone is made up of subzones. These include an automatically created Default Subzone and up to 100 manually configurable subzones. Each manually configured subzone specifies a range of IP addresses. When an endpoint registers with the VCS it is allocated to the appropriate subzone based on its IP address. If the endpoint's IP address does not match any of the subzones, it is assigned to the Default Subzone.

Subzones are used for the purposes of bandwidth management. Once you have set up your subzones you can apply bandwidth limits to:

- individual calls between two endpoints within the subzone
- individual calls between an endpoint within the subzone and another endpoint outside of the subzone
- the total of calls to or from endpoints within the subzone.

The VCS also has a special type of subzone known as the Traversal Subzone. This is a conceptual subzone; no endpoints can be registered to it, but all traversal calls (i.e. calls for which the VCS is taking the media in addition to the signaling) must pass through it. The Traversal Subzone exists in order to allow you to control the amount of bandwidth used by traversal calls, as these can be particularly resource-intensive.

The Local Zone may be independent of network topology, and may be comprised of multiple network segments.

Configuring the Local Zone and its Subzones

The Local Zone and its subzones exist for the purposes of bandwidth management. For full details of how to create and configure subzones, and apply bandwidth limitations to these and the Default Subzone and Traversal Subzone, see the section on Bandwidth Control.

Managing Zones, Neighbors and Alternates

Zones

About Zones

A zone is a collection of endpoints, either all registered to a single system (e.g. VCS, gatekeeper or Border Controller), or of a certain type such as ENUM or DNS. The use of zones enables you to:

- use links to determine whether calls can be made between your local subzones and these other zones
- manage the bandwidth of calls between your local subzones and endpoints in other zones
- more easily search for aliases that are not registered locally
- apply transforms to aliases before searching for them.

Your VCS allows you to configure up to 200 zones of 5 different types. It also has a non-configurable Default Zone.

ENUM Zone

ENUM zones allow you to locate endpoints via an ENUM lookup. You can create one or more ENUM zones based on the ENUM DNS suffix used and/or by pattern matching of the endpoints' aliases.

Once you have configured one or more ENUM zones, you can:

- apply transforms to alias search requests directed to that group of endpoints
- control the bandwidth used for calls between your local VCS and each group of ENUM endpoints.

DNS Zone

DNS zones allow you to locate endpoints via a DNS lookup. You can create one or more DNS zones based on pattern matching of the endpoints' aliases.

Once you have configured one or more DNS zones, you can:

- apply transforms to alias search requests directed to that group of endpoints
- control the bandwidth used for calls between your local VCS and each group of DNS endpoints.

Traversal Client Zone

In order to be able to traverse a firewall, the VCS must be neighbored with a traversal server (for example a TANDBERG Border Controller or another VCS with the Border Controller option enabled).

In this situation your local VCS is a traversal client, so you neighbor with the traversal server by creating a traversal client zone on your local VCS. You then configure it with details of the corresponding zone on the traversal server.

Once you have neighbored with the traversal server you can:

- use the neighbor as a traversal server
- query the traversal server about its endpoints
- apply transforms to any queries before they are sent to the traversal server
- control the bandwidth used for calls between your local VCS and the traversal server.

In order for firewall traversal to work, the traversal server and the traversal client must each be configured with the other's details.

Neighbor Zone

A Neighbor zone could be a collection of endpoints registered to another system (e.g. VCS, gatekeeper, or Border Controller), or it could be a SIP device. The other system is referred to as a neighbor. Neighbors can be part of your own enterprise network, part of a separate network, or even stand-alone systems.

You create a neighbor relationship with the other system by adding it as a neighbor zone on your local VCS. Once you have added it, you can:

- query the neighbor about its endpoints
- apply transforms to any queries before they are sent to the neighbor
- control the bandwidth used for calls between your local VCS and the neighbor zone.

Traversal Server Zone

The VCS may be enabled to act as a traversal server by installing the Border Controller option (contact your TANDBERG representative for further information).

In order to act as a traversal server, the local VCS must be neighbored with each system (e.g. VCS or gatekeeper) that will be its traversal client. To do this, you create a traversal server zone on your local VCS and configure it with the details of the corresponding zone on the traversal client.

Once you have neighbored with the traversal client you can:

- provide firewall traversal services to the traversal client
- query the traversal client about its endpoints
- apply transforms to any queries before they are sent to the traversal client
- control the bandwidth used for calls between your local VCS and the traversal client.

Default Zone

Any incoming calls from endpoints that are not recognized as belonging to any of the existing configured zones are deemed to be coming from the Default Zone.

The VCS comes pre-configured with the Default Zone and default links between it and both the Default Subzone and the Traversal Subzone.

The purpose of the Default Zone is to allow you to manage incoming calls from unrecognized endpoints to the VCS. You can do this by:

- deleting the default links. This will prevent any incoming calls from unrecognized endpoints
- applying pipes to the default links. This will allow you to control the bandwidth consumed by incoming calls from unrecognized endpoints.

The default links can be reinstated at any time via the command:

`xCommand DefaultLinksAdd`

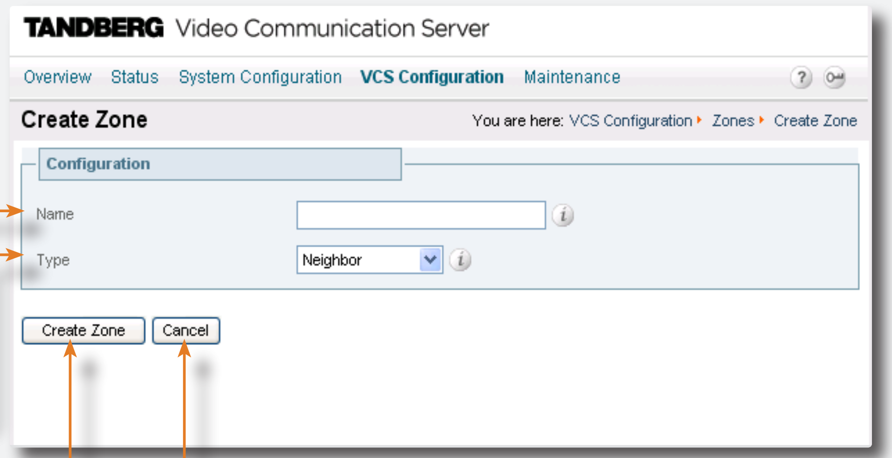
Managing Zones, Neighbors and Alternates

Adding Zones

In order to neighbor with another system (e.g. VCS, gatekeeper or Border Controller) or create an ENUM or DNS zone, you must add a new zone on the local VCS. When adding a new zone you will be asked to specify its Type; this will determine which configuration options will then be available.

To create a new zone:

- *VCS Configuration > Zones.*
  You will be taken to the Zones page.
  Click New.
  You will be taken to the Create Zone page.
- xCommand ZoneAdd



Name

Enter the name you wish to give to this zone. The name acts as a unique identifier, allowing you to distinguish between zones of the same type.

Type

From the Type drop-down menu, select the type of zone you wish to add.

Once the zone has been created, the Type cannot be changed.

Create Zone

Click here to create the zone. You will be taken directly to the Edit Zone page.

Cancel

Click here to return to the Zones page without creating the zone.

Configuring Zones

Once you have created a new zone on the local VCS you must configure it appropriately. For traversal server zones, traversal client zones and neighbor zones this will include providing information about the neighbor system such as IP address and ports.

Zones are configured via the Edit Zone page. You will be taken to this page automatically upon creation of a new zone. To access this page for an existing zone:

- *VCS Configuration > Zones*.
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zone page.
- xConfiguration Zones Zone [1..200]

The sections that follow describe the configuration options available for each zone type.

Configuring Zones - All Types

Name

Assigns a name to the zone. The name acts as a unique identifier, allowing you to distinguish between zones of the same type.

Type

Determines the nature of the specified zone in relation to the Local Zone.

Neighbor: the new zone will be a neighbor of the Local Zone.

TraversalClient: there is a firewall between the zones, and the Local Zone is a traversal client of the new zone.

TraversalServer: there is a firewall between the zones and the Local Zone is a traversal server for the new zone.

ENUM: the new zone contains endpoints discoverable by ENUM lookup.

DNS: the new zone contains endpoints discoverable by DNS lookup.

Once the zone has been created, the Type cannot be changed.

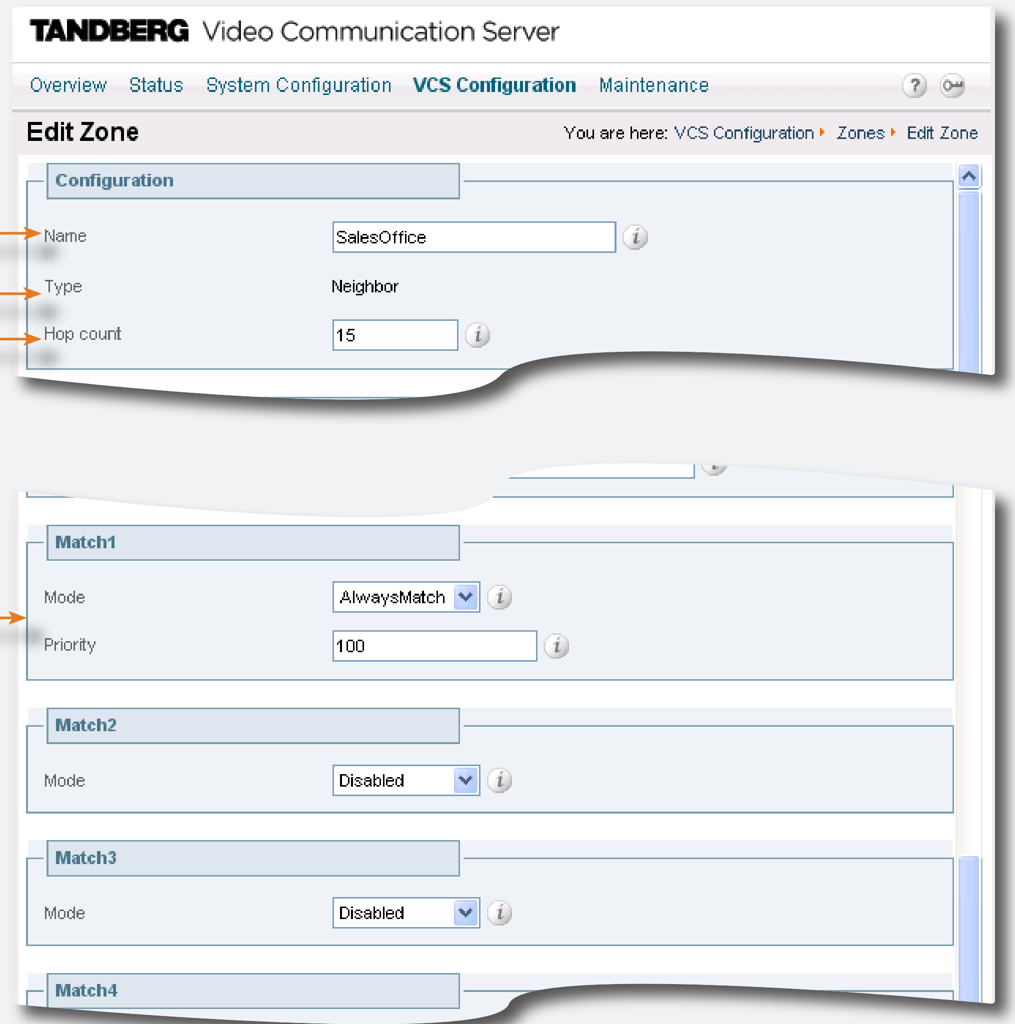
Hop count

The hop count is the number of times a search request will be forwarded to a neighbor gatekeeper or proxy (see Hop Counts for more information). This field specifies the hop count to be used when sending an alias search request to this particular zone.

If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.

Match1 - Match5

The Match sections allow you to configure when and how search requests will be sent to this zone, and also whether any transforms will be applied to aliases being searched for in this zone. These features are described in full in the section Zone searching and alias transforming.



Managing Zones, Neighbors and Alternates

Configuring Neighbor Zones

H.323 mode

Determines whether H.323 calls will be allowed to and from the neighbor zone.

H.323 port

Specifies the port on the neighbor system to be used for H.323 calls to and from the local VCS.

This must be the same port number as that configured on the neighbor system as its H.323 UDP port.

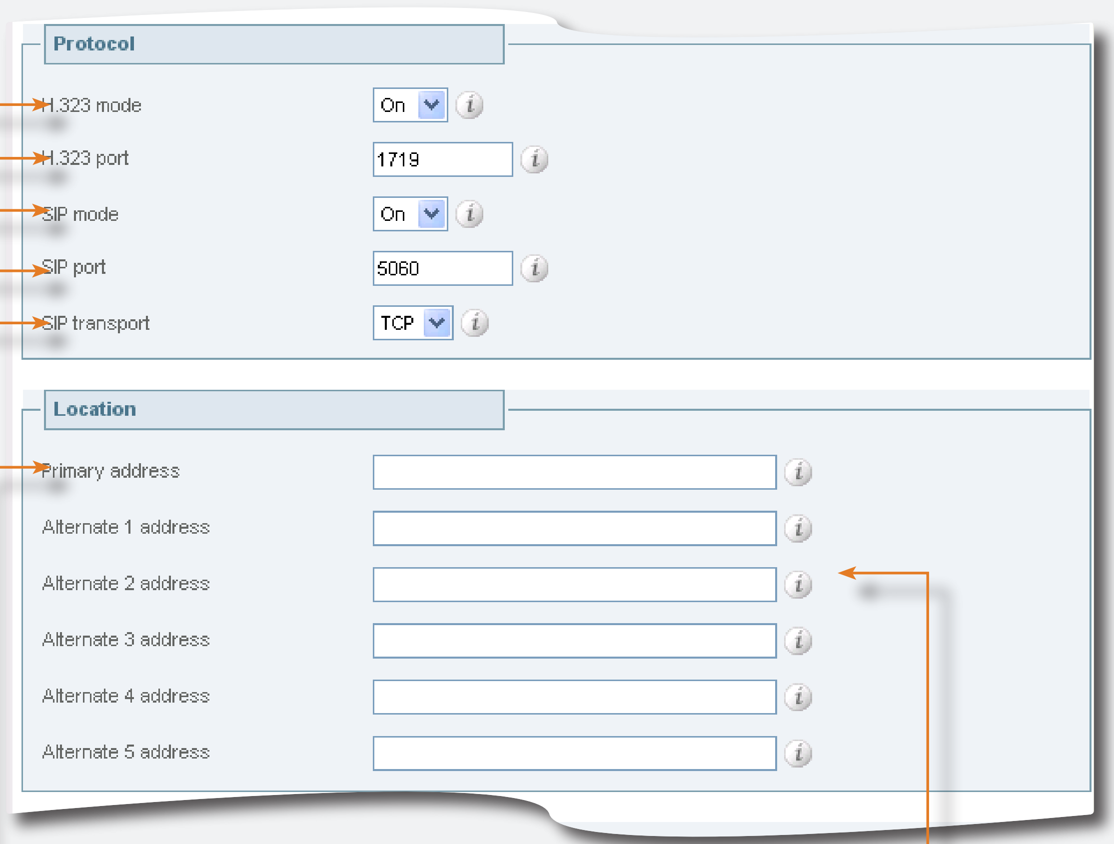
SIP mode

Determines whether SIP calls will be allowed to and from the neighbor zone.

SIP port

Specifies the port on the neighbor system to be used for SIP calls to and from the local VCS.

This must be the same port number as that configured on the neighbor system as its SIP TCP or SIP TLS port (depending on which SIP transport mode is in use).



SIP transport

Determines which transport type will be used for SIP calls to and from the neighbor zone.

Primary address

Enter the IP address or FQDN of the neighbor system.

Alternate 1 to Alternate 5 address

Enter the IP addresses or FQDNs of all Alternates configured on the neighbor system.

Configuring Traversal Client Zones

Retry interval

Specifies the interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried.

H.323 mode

Determines whether H.323 calls will be allowed to and from the traversal server.

H.323 protocol

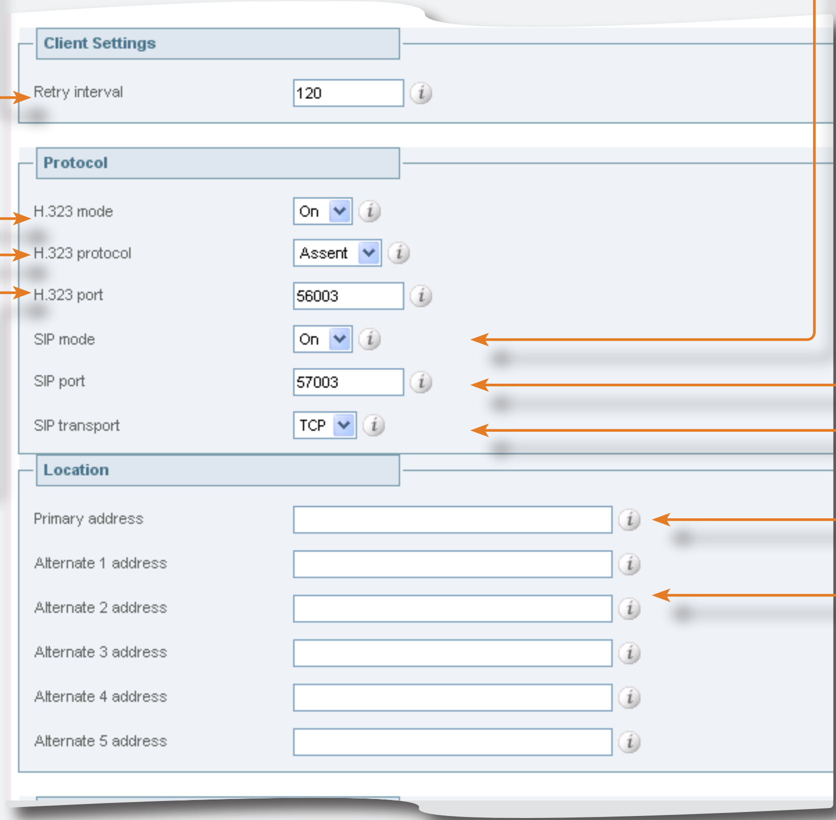
Determines which of the two firewall traversal protocols (Assent or H.460.18) to use for calls to the traversal server. (See Firewall Traversal Protocols for more information.)

H.323 port

Specifies the port on the traversal server to be used for H.323 calls to and from the local VCS.

For firewall traversal to work via H.323, the traversal server must have a traversal server zone configured on it to represent this VCS, using this same port number.

For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see Firewall Traversal.



SIP mode

Determines whether SIP calls will be allowed to and from this zone.

SIP port

Specifies the port on the traversal server to be used for SIP calls to and from the VCS.

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal server.

For firewall traversal to work via SIP, the traversal server must have a traversal server zone configured on it to represent this VCS, using this same transport type and port number.

Primary address

Specifies the IP address or FQDN of the traversal server.

Alternate 1 to Alternate 5 address

Specifies the IP addresses or FQDNs of any alternates configured on the traversal server.

Managing Zones, Neighbors and Alternates

Configuring Traversal Server Zones

There must be an entry in the local VCS's Authentication database for this username. See Authentication for more information.

Authentication username

If the traversal client is a VCS, this is its Authentication Username. If the traversal client is a gatekeeper, this is its System Name.

H.323 mode

Determines whether H.323 calls will be allowed to and from the traversal client.

H.323 protocol

Determines the protocol (Assent or H.460.18) to be used to traverse the firewall/NAT. (See Firewall Traversal Protocols for more information.)

H.323 port

Specifies the port on the local VCS to be used for H.323 calls to and from the traversal client.

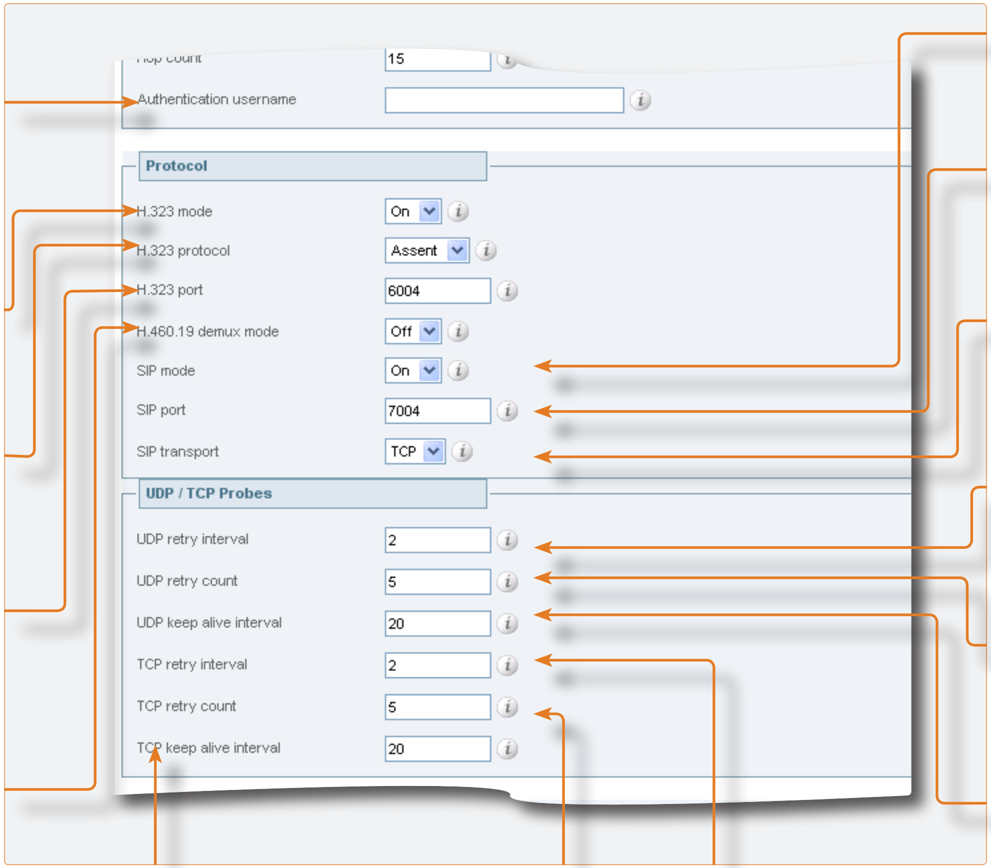
H.460.19 demultiplexing Mode

Determines whether or not the same two ports can be used for media by two or more calls.

On: all calls will use the same two ports.

Off: each call will use a separate pair of ports.

For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see Firewall Traversal.



TCP keep alive interval

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS once a call is established, in order to maintain the firewall's NAT bindings.

TCP retry count

Sets the number of times the client will attempt to send a TCP probe to the VCS Border Controller during call setup.

TCP retry interval

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the VCS during call setup.

SIP mode

Determines whether SIP calls will be allowed to and from this zone.

SIP port

Specifies the port on the local VCS Border Controller to be used for SIP calls to and from the traversal client.

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal client.

UDP retry interval

Sets the frequency (in seconds) with which the client will send a UDP probe to the traversal server if a keep alive confirmation has not been received.

UDP retry count

Sets the number of times the client will attempt to send a UDP probe to the VCS Border Controller during call setup.

UDP keep alive interval

Sets the interval (in seconds) with which the client will send a UDP probe to the VCS Border Controller once a call is established, in order to keep the firewall's NAT bindings open.

The default UDP and TCP probe retry intervals are suitable for most situations. However, if you experience problems with NAT bindings timing out, they may need to be changed.

Configuring ENUM Zones

DNS suffix

Specifies the domain to be appended to the transformed E.164 number to create an ENUM domain for which this zone is queried.

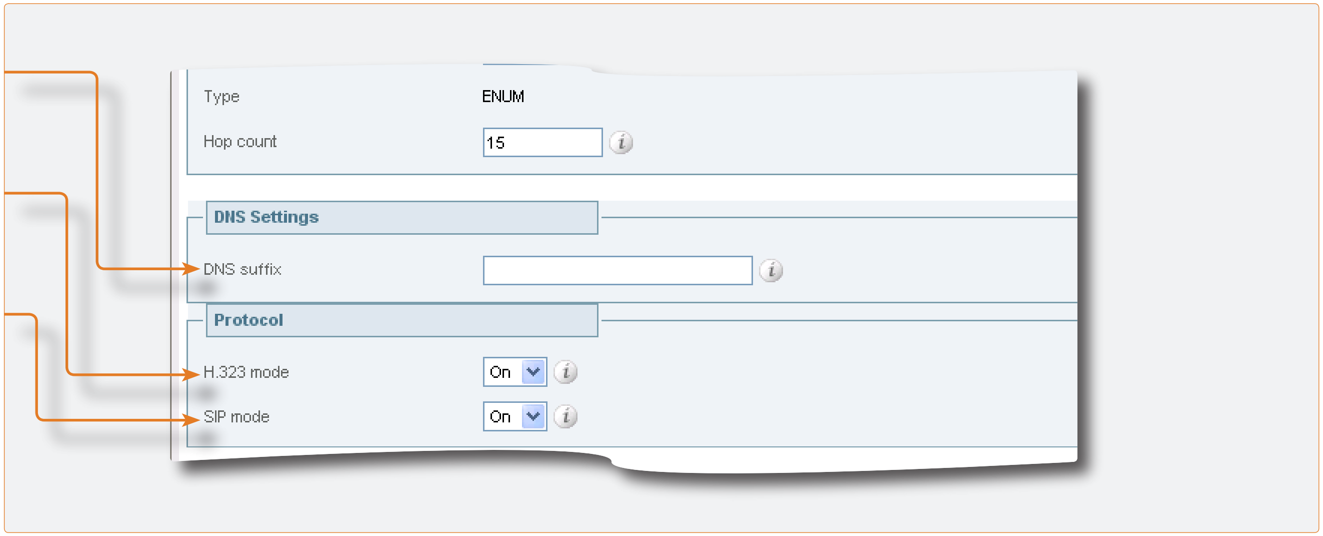
H.323 mode

Determines whether H.323 records will be looked up for this zone.

SIP mode

Determines whether SIP records will be looked up for this zone.

Full details of how to use and configure ENUM zones is given in ENUM Dialing..



Configuring DNS Zones

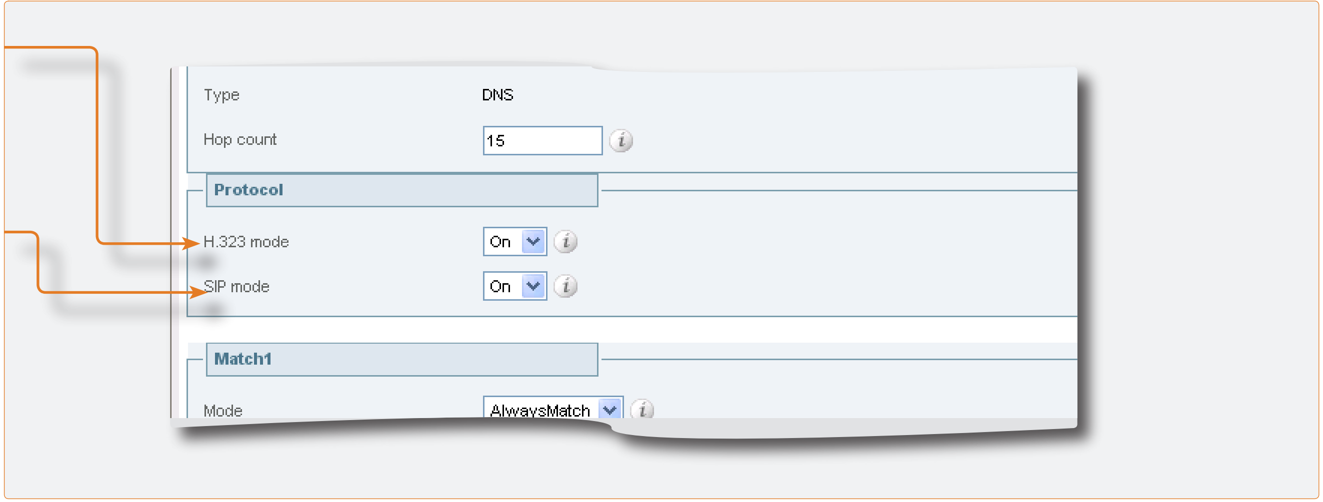
H.323 mode

Determines whether H.323 calls will be allowed to this zone.

SIP mode

Determines whether SIP calls will be allowed to this zone.

Full details of how to use and configure DNS zones is given in URI Dialing.



Managing Zones, Neighbors and Alternates

About Alternates

The purpose of an Alternate is to provide extra reliability.

Each VCS can be part of a pool of up to 6 Alternate VCSs that act as backups to each other in case one becomes unavailable (for example, due to a network or power outage).

All the Alternates in a pool are configured similarly and share responsibility for their endpoint community. When an endpoint registers with the VCS, it is given the IP addresses of all the VCS's Alternates. If the endpoint loses contact with the initial VCS, it will seek to register with one of the Alternates. This may result in your endpoint community's registrations being spread over all the Alternates.

When the VCS receives a Location Request, if it cannot respond from its own registration database, it will query all of its Alternates before responding. This allows the pool of endpoints to be treated as if they were registered with a single VCS.

Alternates are periodically interrogated to ensure that they are still functioning. In order to prevent delays during call setup, any non-functioning Alternates will not receive Location Requests.

Alternates are not used to increase the capacity of your network; they are to provide redundancy. To increase the capacity of your network, add one or more additional VCSs and neighbor them together.

Configuring Alternates

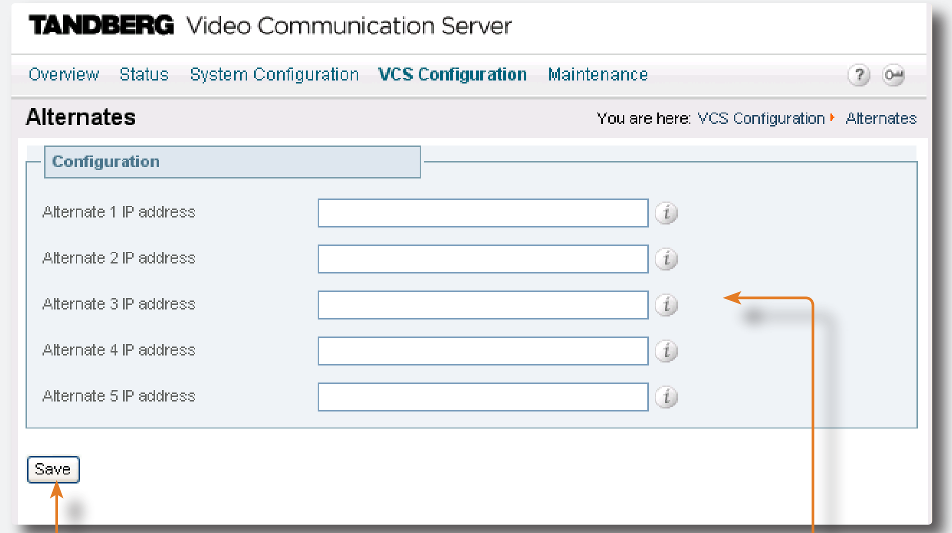
Each VCS can be configured with the IP addresses of up to five other VCSs that will act as Alternates should the current VCS become unavailable.

To configure Alternate VCSs:

- *VCS Configuration > Alternates*.
  You will be taken to the Alternates page.
- `xConfiguration Alternates`

You must configure all Alternates in a pool identically for all registration and call features such as authentication, bandwidth control and policy. If you do not do this, endpoint behavior will vary unpredictably depending on which Alternate it is currently registered with. Alternates should also be deployed on the same LAN as each other so that they may be configured with the same routing information such as local domain names and local domain subnet masks.

When configuring your VCS with the details of the system it will be using as a traversal server, you are given the opportunity to include details of any Alternates of that traversal server. Adding this information to your VCS will ensure that, if the original traversal server becomes unavailable, your VCS can use one of its Alternates instead.



Save

Click Save to save your changes.

Alternate 1 to Alternate 5 IP address

To configure another VCS as an Alternate, enter its IP address. Up to 5 Alternates may be configured.

Setting up a Dial Plan

About Dial Plans

As you start deploying more than one VCS, it is useful to neighbor the systems together so that they can query each other about their registered endpoints. Before you start, you should consider how you will structure your dial plan. This will determine the aliases assigned to the endpoints, and the way in which the VCSs are neighbored together. The solution you chose will depend on the complexity of your system. Some possible options are described below.

Flat Dial Plan

The simplest approach is to assign each endpoint a unique alias and divide the endpoint registrations between the VCSs. Each VCS is then configured with all the other VCS as neighbor zones. When one VCS receives a call for an endpoint which is not registered with it, it will send out a Location Request to all the other neighbor VCSs.

Whilst conceptually simple, this sort of flat dial plan does not scale very well. Adding or moving a VCS requires changing the configuration of every VCS, and one call attempt can result in a large number of location requests. This option is therefore most suitable for a deployment with just one or two VCSs and its Alternates.

Structured Dial Plan

An alternative deployment would use a structured dial plan whereby endpoints are assigned an alias based on the system they are registering with.

If you are using E.164 aliases, each VCS would be assigned an area code. When the VCSs are neighbored together, each neighbor zone is configured with its corresponding area code as a prefix (i.e. a Match Mode of Pattern and a Type of Prefix). That neighbor will now only be queried for calls to numbers which begin with its prefix.

In a URI based dial plan, similar behavior may be obtained by configuring neighbors with a suffix to match the desired domain name.

It may be desirable to have endpoints register with just the subscriber number -- the last part of the E.164 number. In that case, the VCS could be configured to strip prefixes before sending the query to that zone.

A structured dial plan will minimize the number of queries issued when a call is attempted. However, it still requires a fully connected mesh of all VCSs in your deployment. A hierarchical dial plan can simplify this.

Hierarchical Dial Plan

In this type of structure one VCS is nominated as the Directory for the deployment, and all other VCSs are neighbored with it alone. Each VCS is configured with the Directory VCS as a neighbor zone with a Match Mode of Always, and the Directory VCS is configured with each VCS as a neighbor zone with a Match Mode of Pattern and its prefix as the Pattern String.

There is no need to neighbor the VCSs with each other. Adding a new VCS now only requires changing configuration on that system and the Directory VCS.

However, failure of the Directory VCS in this situation could cause significant disruption to communications. Consideration should be given to the use of Alternates for increased resilience.

Locating a Destination Endpoint

Overview

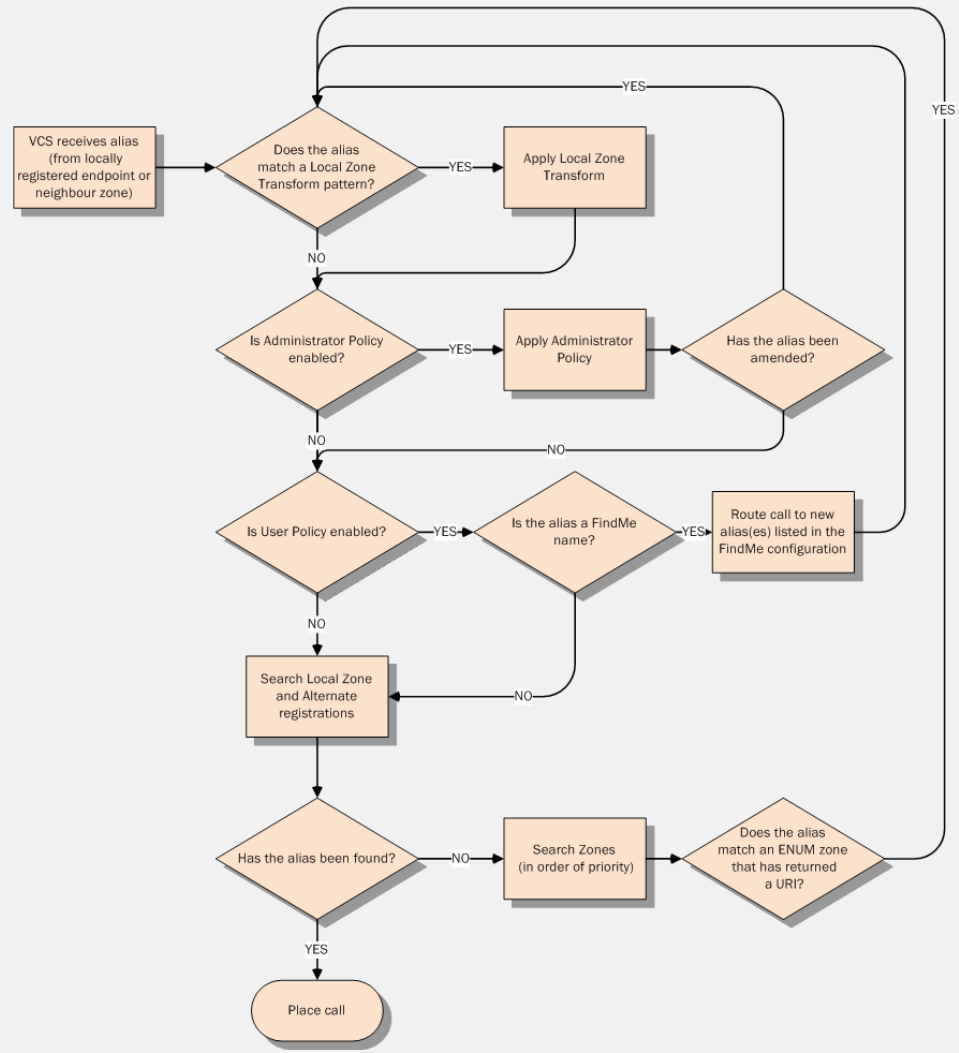
One of the functions of the VCS is to route calls to their appropriate destination, based on the address or alias received by a locally registered endpoint or neighbor zone.

There are a number of steps involved in determining the destination of a call, and some of these steps can involve transforming the alias or redirecting the call to other aliases. It is important to understand the process before setting up your dial plan so you can avoid circular references.

Process

The process followed by the VCS when attempting to locate a destination endpoint is shown in the diagram opposite.

1. The user enters into their endpoint the an alias or address of the destination endpoint. This can be in a number of different formats.
2. The destination address is sent from the caller's endpoint to its local VCS (i.e. the VCS to which it is registered).
3. The VCS applies any Local Zone transforms to the alias.
4. The VCS applies any Administrator Policy to the (transformed) alias. If this results in a new alias, the process starts again, with the new alias checked against the Local Zone transforms.
5. The VCS applies any User Policy to the alias. If the alias is a FindMe name, the process will start again; all the resulting aliases will be checked against Local Zone transforms and Administrator Policy.
6. The VCS then checks all its local registrations and those of its Alternates for the alias, placing the call if the alias is found.
7. If the alias is not found locally, the VCS will then query its zones, in priority order, to see if any of them can find the alias. If the alias matches an ENUM zone, this may return a URI. If so, the process starts again; the URI is checked against any Local Zone transforms, Administrator Policy and User Policy.
8. If the alias is found by one of the neighbor zones, the call will be placed to that zone.



Dialing by Address Types

About the Different Address Types

The destination address that is entered via the caller's endpoint can take a number of different formats, and this will affect the specific process that the VCS follows when attempting to locate the destination endpoint. The address types supported by the VCS are:

- IP address e.g. `10.44.10.1` or `3ffe:80ee:3706::10:35`
- H.323 ID e.g. `john.smith` or `john.smith@example.com`
- E.164 alias e.g. `441189876432` or `6432`
- URI e.g. `john.smith@example.com`
- ENUM e.g. `441189876432` or `6432`

Each of these address types may require some configuration of the VCS in order for them to be supported. The following sections describe the configuration required for each address type.

We recommend that endpoints register with an H.323 ID that is in the form of a URI.

Dialing by IP Address

Dialing by IP address is necessary when the destination endpoint is not registered with any system (e.g. VCS, gatekeeper or Border Controller). If the destination endpoint is registered with one of these systems, then it may still be possible to call it using its IP address but we recommend that one of the other addressing schemes should be used instead as they are more flexible.

In order to make a call by dialing the destination endpoint's IP address, the call must be able to be routed via a VCS that is configured with a Calls to Unknown IP Addresses setting of Direct. This could be the local VCS, or it could be one of its neighbors (in which case the local VCS would route the call to the neighbor, which would then place the call directly to the IP address).

However, if the destination IP address is found in a local subzone (i.e. it is an endpoint registered to the same VCS as the endpoint making the call), then the call will be placed regardless of the Calls to Unknown IP Addresses setting.

Endpoints registered to a VCS Border Controller

Calls made by dialing the IP address of an endpoint registered directly with a VCS Border Controller will be forced to route through the VCS Border Controller. The call will therefore be subject to any restrictions configured on that system.

If you are calling from an unregistered endpoint, we do not recommend dialing the destination endpoint using its IP address. The presence of a firewall may disrupt the call. Instead place the call to the VCS to which the destination endpoint is registered as described in Calls from an Unregistered Endpoint.

Dialing by H.323 ID or E.164 alias

No special configuration is required in order to place a call using an H.323 ID or E.164 alias. The VCS follows the usual process and searches for the ID or alias among its local registrations and those of its Alternates. If no match is found, it may forward the query on to its neighbors, depending on the match and priority settings of each.

Dialing by H.323 or SIP URI

When a user places a call using URI dialing, they will typically dial name@example.com.

URI dialing makes use of DNS to locate the destination endpoint. In order to support URI dialing on the VCS you must configure it with at least one DNS server and at least one DNS zone,

Full instructions on how to configure the VCS to support URI dialing (both outbound and inbound) are given in URI Dialing.

Dialing by ENUM

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias. The E.164 number is converted into a URI by the DNS system, and the rules for URI dialing are then followed to place the call.

The ENUM dialing facility allows you to retain the flexibility of URI dialing whilst having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing via a numeric keypad.

In order to support ENUM dialing on the VCS you must configure it with at least one DNS server and the appropriate ENUM zone(s).

Full instructions on how to configure the VCS to support ENUM dialing (both outbound and inbound) are given in ENUM Dialing.

Hop Counts

About Hop Counts

Each search request is assigned a hop count value by the system that initiates the search. Every time the request is forwarded to another neighbor gatekeeper or proxy, the hop count value is decreased by a value of 1. When the hop count reaches 0, it will not be forwarded on any further.

The hop count used in search requests initiated by the local VCS is configurable on a zone-by-zone basis. This value will apply to search requests originating from the local VCS and sent to that zone. It will also override any existing hop counts in requests being forwarded to that zone if the original hop count is higher (if the hop count is lower than that set for the zone, the lower value will apply).

For H.323, the hop count only applies to search requests. For SIP, the hop count applies to all requests sent to a zone, affecting the Max-Forwards field in the request.

The hop count value can be between 1 and 255.
The default is 15.

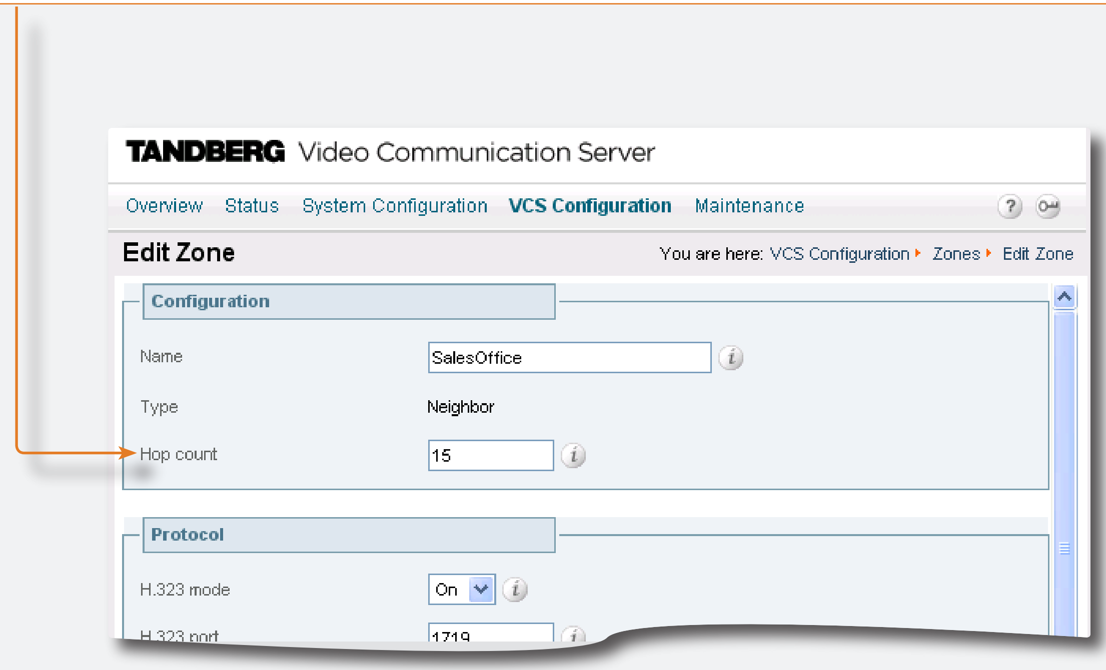
When dialing by URI or ENUM, the hop count used is that for the associated DNS or ENUM zone via which the destination endpoint was found.

Configuring Hop Counts

To configure the hop count for a zone:

- *VCS Configuration > Zones.*
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zone page.
  In the Configuration section, in the Hop Count field, enter the hop count value you wish to use for this zone.
- `xConfiguration Zones Zone [1..200] HopCount`

For full details on other zone options, see Configuring Zones.



Overview

About Administrator Policy

The VCS allows you to set up a set of rules to control which calls are allowed, which are rejected, and which are to be redirected to a different destination. These rules are known as Administrator Policy.

If Administrator Policy is enabled and has been configured, each time a call is made the VCS will execute the policy in order to decide, based on the source and destination of the call, whether to

- proxy the call to its original destination
- redirect the call to a different destination
- reject the call.

You can set up an Administrator Policy in either of two ways:

- by configuring basic administrator policy using the web interface. (Note that this will only allow you to Allow or Reject specified calls)
- by uploading a script written in the Call Processing Language (CPL).

Only one of these two methods can be used at any one time to specify Administrator Policy. If a CPL script has been uploaded, this will disable use of the web interface to configure administrator policy. In order to use the web interface, you must delete the CPL script that has been uploaded.

When enabled, Administrator Policy is executed for all calls going through the VCS.

Use Administrator Policy to determine which callers can make or receive calls via the VCS. Use Allow and Deny lists to determine which aliases can or cannot register with the VCS.

Administrator Policy and Authentication

Administrator Policy uses the source and destination of a call to determine the action to be taken. Policy interacts with Authentication when considering the source alias of the call. If your VCS is part of a secure environment, any policy decisions based on the source of the call should only be made when that source can be authenticated. Whether or not the VCS considers an endpoint to be authenticated depends on the Authentication Mode setting of the VCS.

Authentication Mode On

When Authentication Mode is set to On on the VCS, all endpoints and neighbors are required to authenticate with it before calls will be accepted. In this situation, the VCS acts as follows:

An endpoint is considered to be authenticated when:

- it is a locally registered endpoint. (Because Authentication Mode is On, the registration will have been accepted only after the endpoint authenticated successfully with the VCS.)
- it is a remote endpoint that is registered to and authenticated with a Neighbor VCS, and that Neighbor in turn has authenticated with the local VCS.

An endpoint is considered to be unauthenticated when:

- it is a remote endpoint registered to a neighbor and that neighbor has not authenticated with the VCS. This is regardless of whether or not the endpoint authenticated with the neighbor.

If a call is received from an unauthenticated neighbor or endpoint the call's source aliases will be removed from the call request and replaced with an empty field before the Administrator Policy is executed. This is because there is a possibility that the source aliases could be forged and therefore they should not be used for policy decisions in a secure environment. This means that, when Authentication Mode is On and you configure policy based on the source alias, it will only apply to authenticated sources.

Authentication Mode Off

When Authentication Mode is set to Off on the VCS, calls will be accepted from any endpoint or neighbor. The assumption is that the source alias is trusted, so authentication is not required.

Administrator Policy

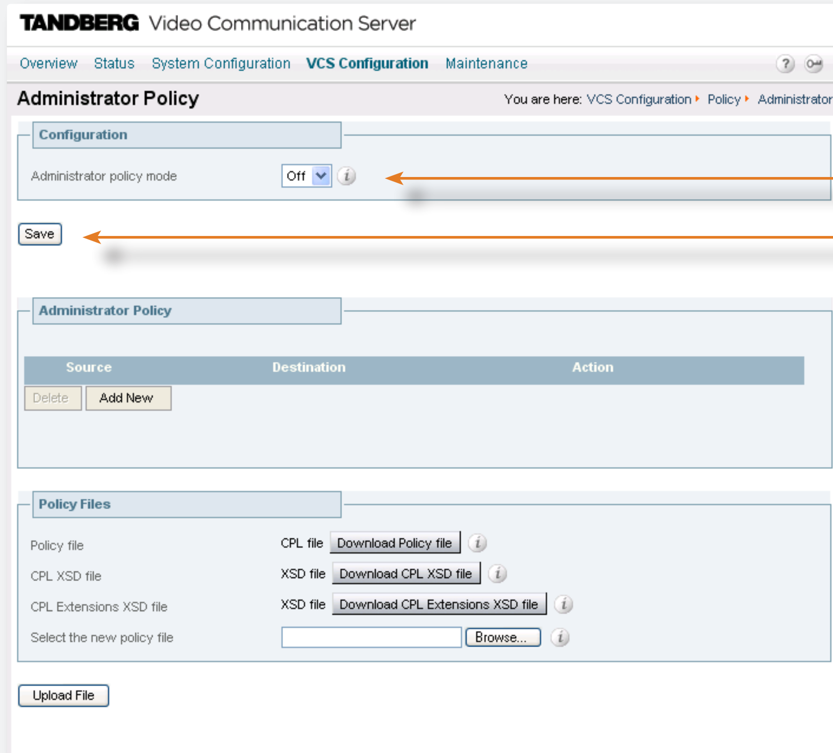
Enabling the use of Administrator Policy

To enable Administrator Policy:

- *VCS Configuration > Policy > Administrator*. You will be taken to the Administrator Policy page.
- `xConfiguration Policy AdministratorPolicy Mode`

Once you have enabled the use of Administrator Policy, you must define the policy to be used. This is done either via the web interface or by uploading a CPL script.

If Administrator Policy is on but a policy has not been configured, then a default policy will be applied that allows all calls, regardless of source or destination.



Administrator Policy Mode

On: Administrator Policy is enabled. If a CPL script has been uploaded, this policy will be used. Otherwise, the policy configured via the Administrator Policy section will be used.

Off: Administrator Policy is not in use.

Save

You must click here for any changes to the Administrator Policy Mode to take effect.

Administrator Policy

Configuring Administrator Policy via the Web Interface

To configure Administrator Policy using the web interface:

- *VCS Configuration > Policy > Administrator*. You will be taken to the Administrator Policy page.

You will not be able to use the web interface to configure Administrator Policy if a CPL file is already in place. If this is the case, you will have the option to Delete Existing file. Doing so will delete the existing Administrator Policy and enable use of the web interface for Administrator Policy configuration.

Administrator Policy

This section shows the web-configured Administrator policy currently in place.

Delete

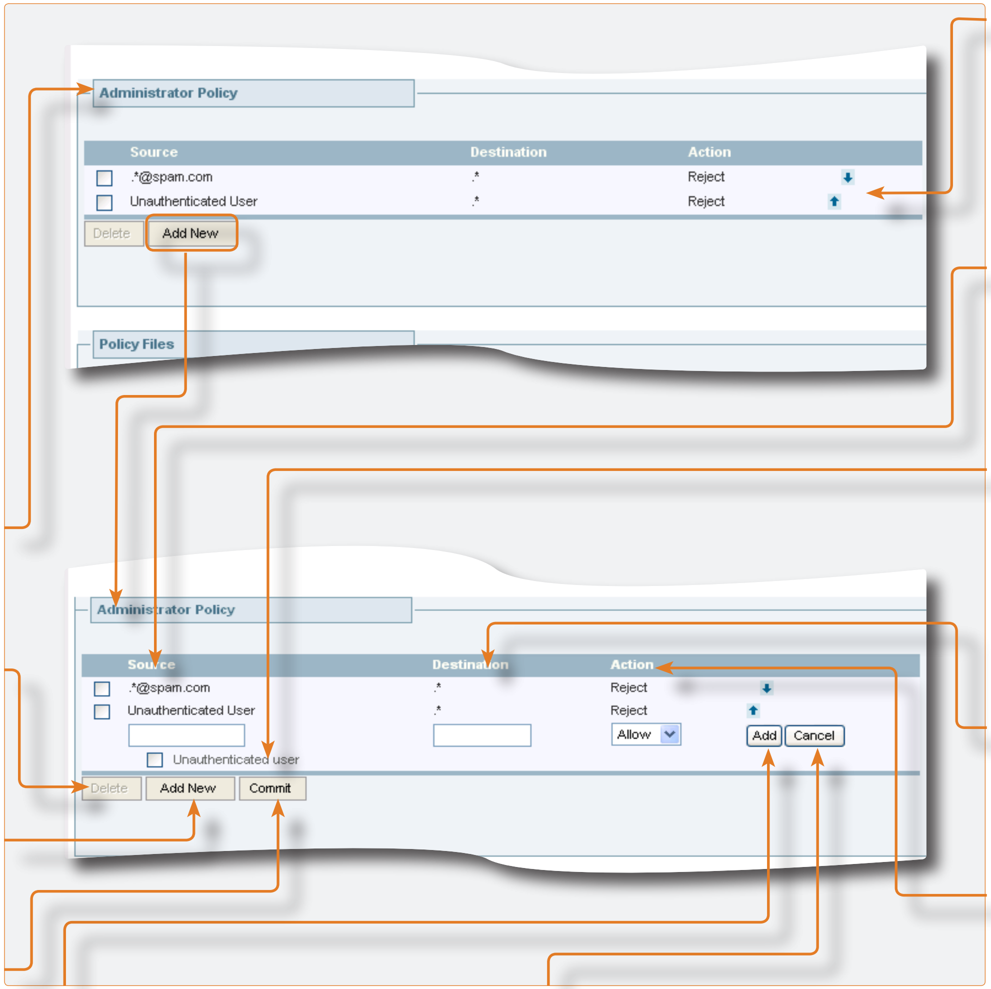
To remove one or more line items from the list, check the box to the left of the item and then click Delete.

Add New

Click to add the new item to the Policy. A new row with empty fields for you to complete will appear.

Commit

Updates the existing Administrator Policy with the changes you have made.



Add

Adds the new item to the Administrator Policy.

Cancel

Returns to the Administrator Policy page without adding the new item.

Order

Each combination of Source and Destination is compared, in the order shown, with the details of the call being made until a match is found. To move a particular item to higher or lower in the list, click on the ↑ and ↓ icons respectively.

Source

The alias that the calling endpoint used to identify itself when placing the call. This field supports Regular Expressions.

Unauthenticated user

Check this box if you wish the new policy to apply to all incoming calls where the endpoint making the call is not either:

- locally registered and authenticated with the VCS, or
- registered and authenticated to a neighbor which in turn has authenticated with the local VCS.

Destination

The alias that the endpoint dialled to make the call. This field supports Regular Expressions.

Action

Whether or not the call will be permitted.

Allow: if both the Source and Destination aliases match those listed, call processing will continue.

Reject: if both the Source and Destination aliases match those listed, the call will be rejected.

Administrator Policy

Configuring Administrator Policy via a CPL script

Uploading a CPL Script

You can use CPL scripts to configure advanced Administrator Policy. To do this, you must first create and save the CPL script as a text file, after which you upload it to the VCS.

The CPL script cannot be uploaded via the command line interface.

About CPL XSD files

The CPL script must be in a format supported by the VCS. The Administrator Policy page allows you to download the XML schemas which are used to check the script before it is uploaded to the VCS, so you can check in advance that your CPL script is valid.

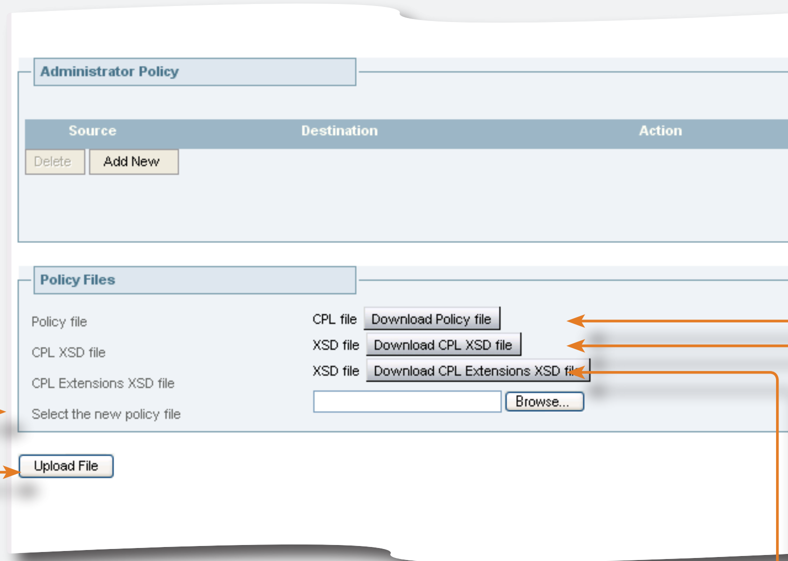
Select the new policy file

Enter the file name or Browse to the CPL script you wish to upload.

Upload File

Once you have selected the file containing the CPL script, click here to upload it to the VCS.

For information on the CPL syntax and commands that are supported by the VCS, see CPL Reference.



Downloading policy files

Download Policy file

Click here to download the Administrator Policy that is currently in place, as an XML-based CPL script.

- if Administrator Policy has been configured using a CPL script, this will show you the script that was uploaded
- if Administrator Policy has been configured using the web interface, this will show you the CPL version of the policy
- if Administrator Policy is On but a policy has not been configured, this will show you the default CPL script that allows all calls.

You may wish to download the file in order to take a backup copy of the Administrator Policy, or you may want to use the web-configured Administrator Policy as a starting point for a more advanced CPL script.

If you download a web-configured Administrator policy as a CPL script and then upload it back to the VCS without editing it, the VCS will recognise the file and automatically add each rule back into the Administrator Policy section of the web interface.

Download CPL XSD file

Downloads the XML schema used for the CPL script.

Download CPL Extensions XSD file

Downloads the XML schema used for additional CPL elements supported by the VCS.

About User Policy

What is User Policy?

User Policy is the set of rules that determines what happens to a call for a particular user or group when it is received by the TANDBERG VCS.

The VCS's User Policy is based on the use of TANDBERG's FindMe™. This feature lets you assign a single "FindMe" name to individuals or groups in your enterprise. Users can determine which devices will be called when their FindMe name is dialled, and can also specify what happens if those devices are busy or go unanswered.

The FindMe feature means that potential callers can be given a single FindMe Alias on which they can contact an individual or group in your enterprise - callers won't have to know details of all the devices on which that person or group might be available.

Process Overview

When the VCS receives a call for a particular alias, it checks to see whether User Policy has been enabled. If so, the VCS queries the User Policy Manager to see whether that alias is listed as a FindMe name. If so, the call is forwarded to the endpoints according to the User Policy set up for that FindMe alias.

If User Policy has not been enabled, or the alias is not present in the User Policy Manager, the VCS will continue to search for the alias in the usual manner, i.e. first locally and then sending the request out to neighbors.

User Policy is invoked after any Administrator Policy configured on the VCS has been applied.

Recommendations When Deploying FindMe

- The FindMe name should be in the form of a URI, and should be the individual's primary URI.
- Endpoints should not register with an alias that is the same as an existing FindMe name. You can prevent this by including all FindMe names on the Deny List.

For example, users at Example.com would have a FindMe name in the format john.smith@example.com. Each of their endpoints would be registered in a slightly different format, for example their office endpoint would be registered with the alias john.smith.office@example.com; their home endpoint as john.smith.home@example.com and their Movi name as john.smith.movi@example.com. Each of these endpoints can then be included in the list of devices to ring when the FindMe name is called.

How are Devices Specified?

When configuring their FindMe account, users are asked to specify the devices to which calls to their FindMe name will be routed.

While it is possible to specify aliases and even other FindMe names as one of the devices, we recommend that this is not done. Instead we recommend that users specify the physical devices they wish to ring when their FindMe name is called.

Who Must do What Before FindMe™ Can Be Used?

FindMe™ is an optional feature on the VCS, and you must install the appropriate option key before it can be used. Contact your TANDBERG representative for more information.

The following steps are required for the use of FindMe one the option has been installed:

1. The VCS administrator enables and configures User Policy.
2. The VCS administrator creates a user account for each user or group who require a FindMe name.
3. The owner of the FindMe name configures their account settings.

User Policy Manager

The User Policy Manager is the application that manages the FindMe user accounts.

The VCS has its own User Policy Manager. However, you also have the option to use a User Policy Manager on a remote system.

User Policy

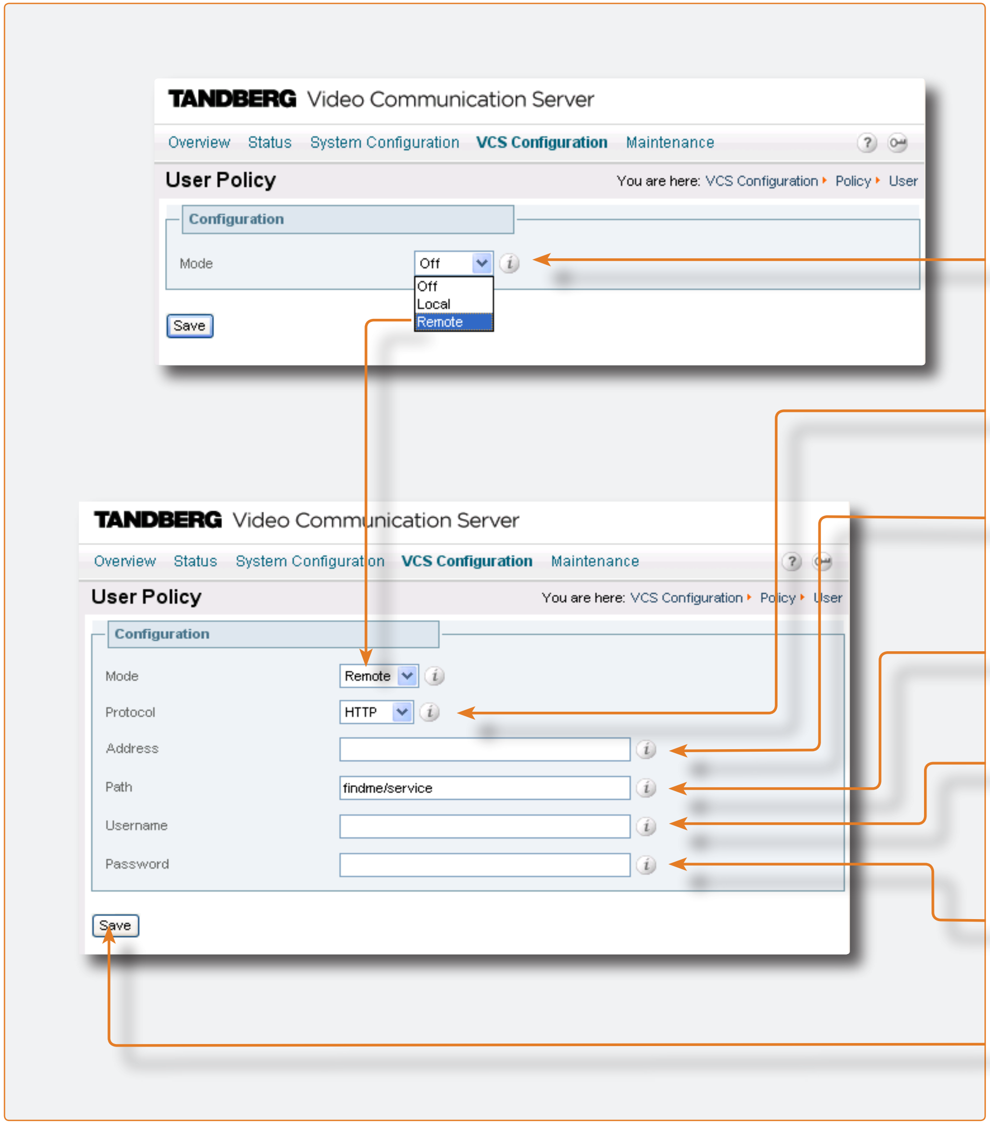
Enabling User Policy on the VCS

Configuring User Policy Manager

To configure the User Policy Manager:

- *VCS Configuration > Policy > User*.
  You will be taken to the User Policy page.
- xConfiguration Policy UserPolicy

Administrator Policy will always be applied regardless of the User Policy mode.



Mode

Determines whether or not User Policy will be enabled, and if so, the location of the User Policy Manager.

Off: User Policy is not enabled.

Local: User Policy is enabled and the VCS's own User Policy Manager is used.

Remote: User Policy is enabled and a User Policy Manager located on another system is used. If you select this option, further configuration options will appear (see below).

Protocol

The protocol used to connect to the remote User Policy Manager.

Address

The IP address or domain name of the remote User Policy Manager.

Path

The URL of the remote User Policy Manager.

Username

The username used by the VCS to log in and query the remote User Policy Manager.

Password

The password used by the VCS to log in and query the remote User Policy Manager.

Save

Click here to save your changes.

User Policy

Managing FindMe User Accounts

About User Accounts

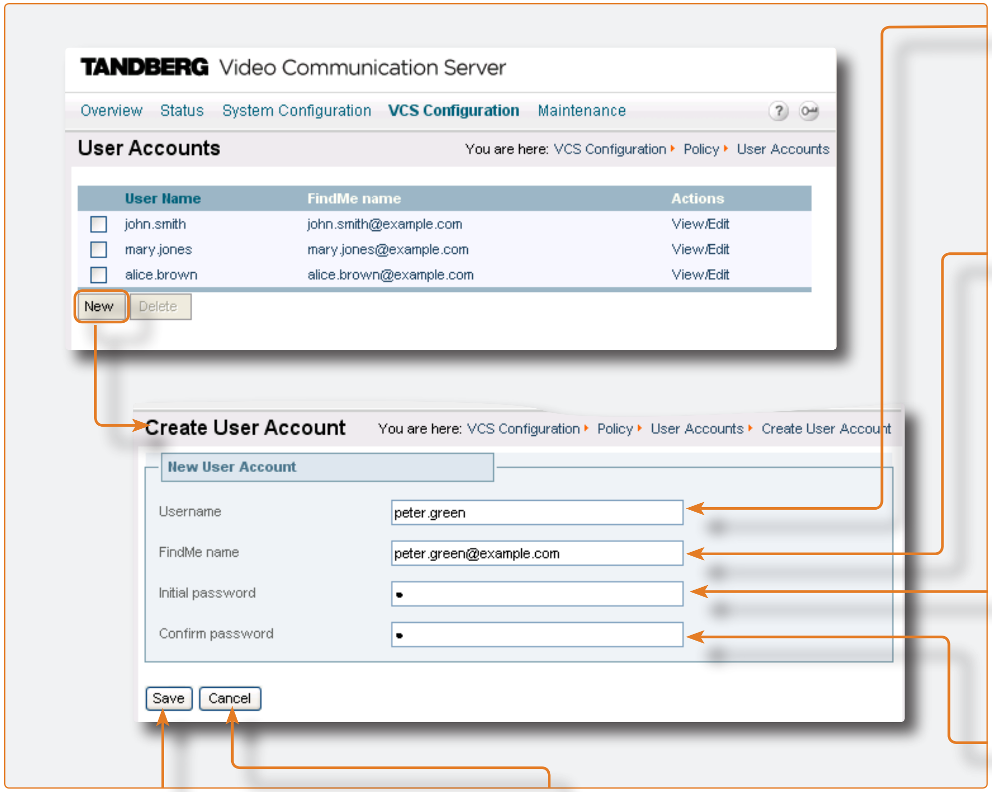
FindMe user accounts must be created by the VCS Administrator before they can be accessed and configured by users.

Each user account is accessed via a username and password associated with a specific FindMe name.

Creating a New User Account

- *VCS Configuration > Policy > User Accounts*.
  You will be taken to the User Accounts page.
  Select New.
  You will be taken to the Create User Account page.

Once a new account has been created, calls to the FindMe name for that account will be rejected until one or more devices have been configured for that account.



Username

The name of the user for whom you are creating an account. This is the name they will use to log in when configuring their FindMe options.

FindMe name

The FindMe name on which the user can be contacted.

The FindMe name can be any string of up to 60 characters. However, not all endpoints are able to dial aliases with spaces or other non-alphanumeric characters so we recommend that these are not used in your FindMe names.

Initial password

The password to be used along with the Username when logging into this account.

Confirm password

Retype the password.

Save

Click here to create the new account and return to the User Accounts page.

Cancel

Click here to return to the User Accounts page without creating the new account,

User Policy

Managing FindMe User Accounts

Changing a User Password

You can change a password on behalf of a user without knowing their existing password. This is useful when the user has forgotten their password.

To change the password:

- *VCS Configuration > Policy > User Accounts*.
  You will be taken to the User Accounts page.
  Click on the user account whose password you wish to change.
  You will be taken to the Edit User Account page.

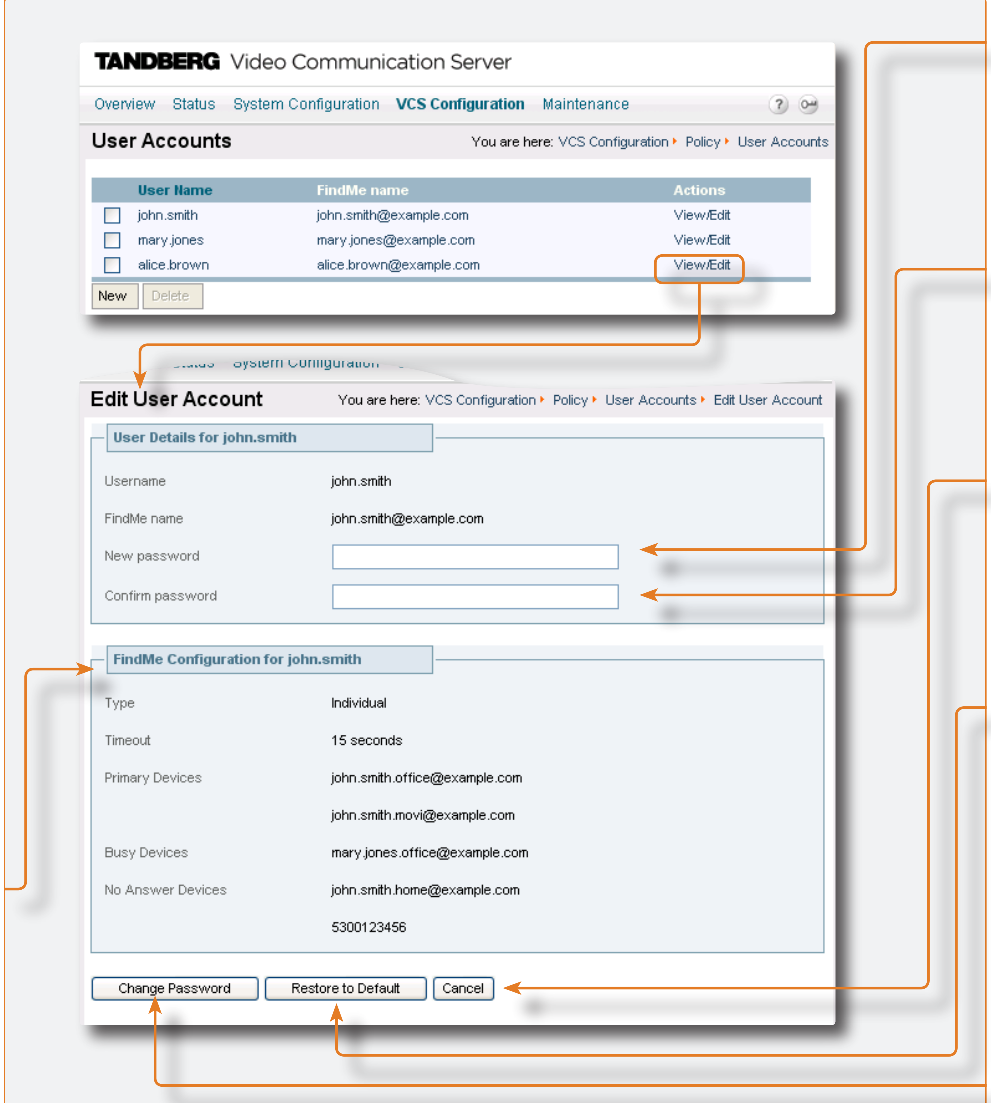
Viewing Existing User Account Settings

To view the configuration of an existing user account:

- *VCS Configuration > Policy > User Accounts*.
  You will be taken to the User Accounts page.
  Click on the user account whose password you wish to change.
  You will be taken to the Edit User Account page.

FindMe Configuration for...

This section shows you the current configuration for the user.



New password

Type the new password to be used along with the Username when logging into this account.

Confirm password

Retype the new password.

Cancel

Click here to return to the User Accounts page without changing the password,

Restore to Default

Click here to delete any existing configuration for this FindMe name. This will have the effect that any calls to that FindMe name will be rejected until one or more devices are reconfigured for that account.

Change Password

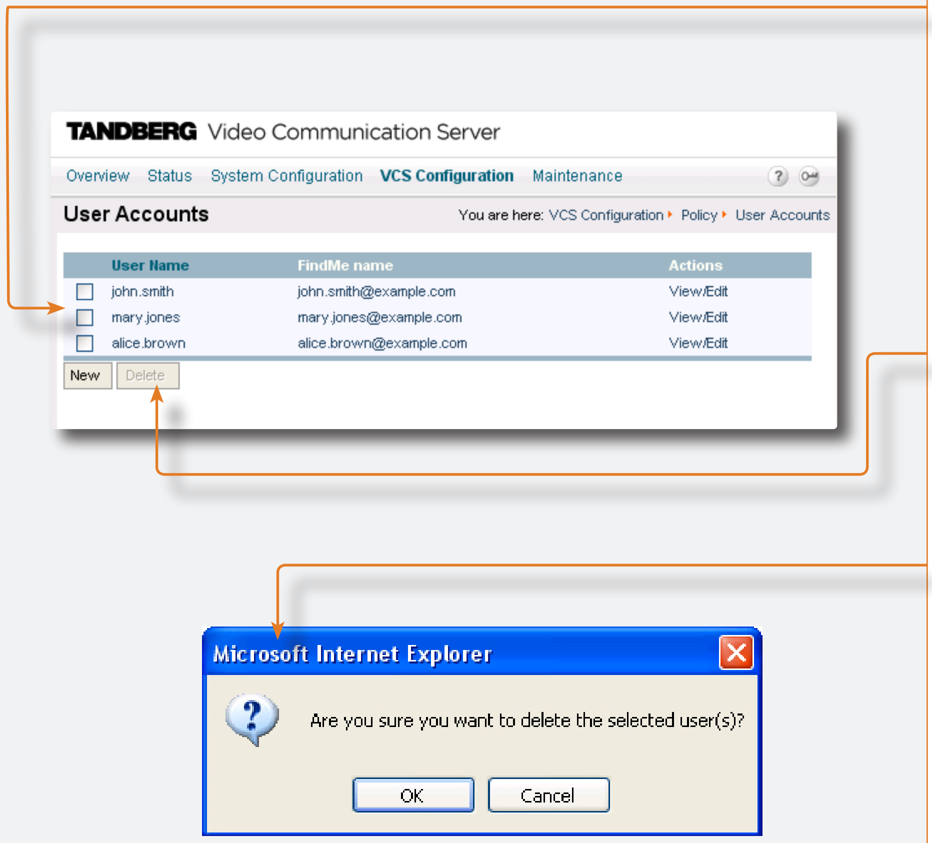
Click here to update the password and return to the User Accounts page.

Managing FindMe User Accounts

Deleting a User Account

To change delete a FindMe user account:

- *VCS Configuration > Policy > User Accounts*. You will be taken to the User Accounts page.



Tick the box next to the account you wish to delete.

Delete

Click here to delete the selected accounts.

Are you sure...?

A confirmation window will appear to ensure that you wish to proceed. Click OK to continue.

About your FindMe User Account

About FindMe™

The FindMe feature allows you as an individual or part of a group to have a single name on which you can always be called, and you chose where calls to that name will be routed. You can also determine what happens if your first choices are either busy or unanswered after a certain period of time.

For example, you could set up your individual FindMe name so that it will call you on your desktop videophone first. If there's no answer after 10 seconds it will divert the call to your mobile phone, and if your desktop phone is busy it will divert the call to your colleague's desktop videophone.

Alternatively, you could have a single FindMe name for your team, and set it up so that all the team member's desktop videophones will ring when anyone calls the FindMe name.

FindMe User Accounts

Each FindMe name has an associated user account. Your FindMe user account is set up by your system administrator. Once this has been done, you can log in to your account via a web interface and configure it with details of the device(s) on which you want to be contacted:

- when a call is first placed to your FindMe name
- if any or all of your first choice of devices are busy
- if all of your first choice of devices are unanswered

You can update these details as often as you wish.

Individual versus Group FindMe

There are two types of FindMe names: individual and group.

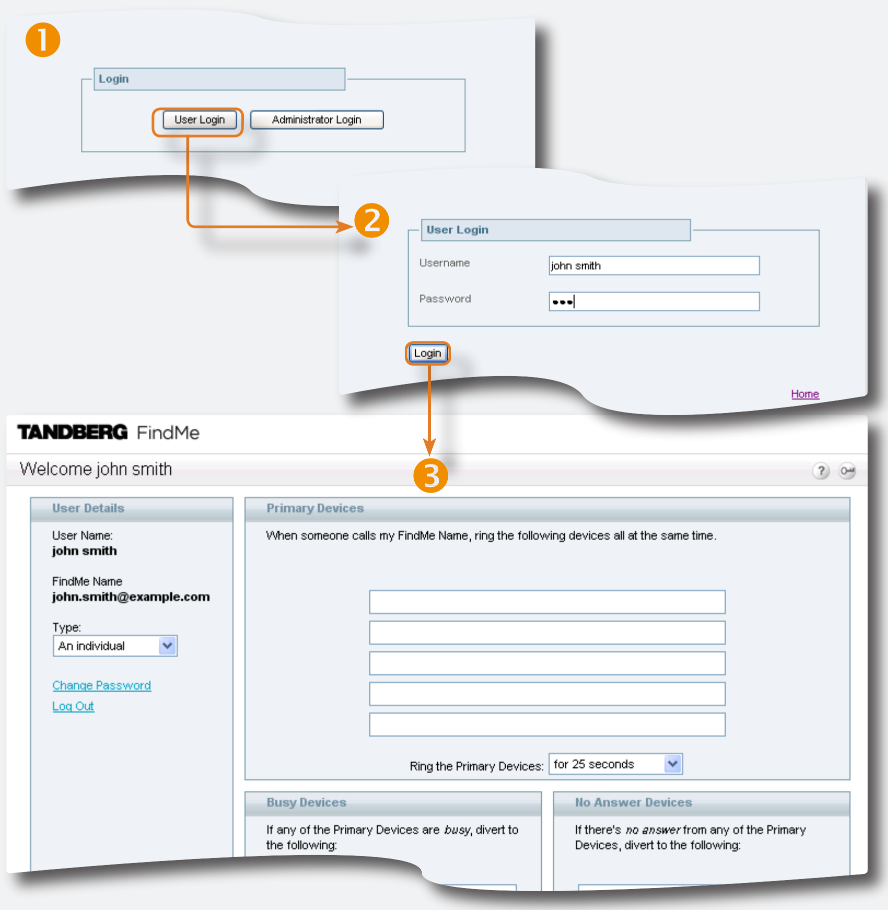
The only difference between the two is what happens if one of the devices in the initial list is busy.

For individuals, it is assumed that you will only be able to take calls on one device at a time, therefore if any devices in your Primary list are busy, the call will immediately divert to the device(s) in your Busy list.

For groups, it is assumed that more than one person is available to take calls, so the call will only divert to the device(s) in the Busy list if all devices in the Primary list are engaged.

Accessing the FindMe Configuration Page

To configure your FindMe user account, you must log in via a web browser, as described below:



1. Go to the FindMe link provided to you by your system administrator.

   This will take you to the Login page.

   Select User Login.

2. Enter the Username and Password provided to you by your System Administrator.

   Select Login.

3. You will be taken to the FindMe page.

   From here you can configure your FindMe options as either an individual or a group.

Configuring your FindMe User Account

If no devices are configured for a FindMe name, all calls to that name will be rejected.

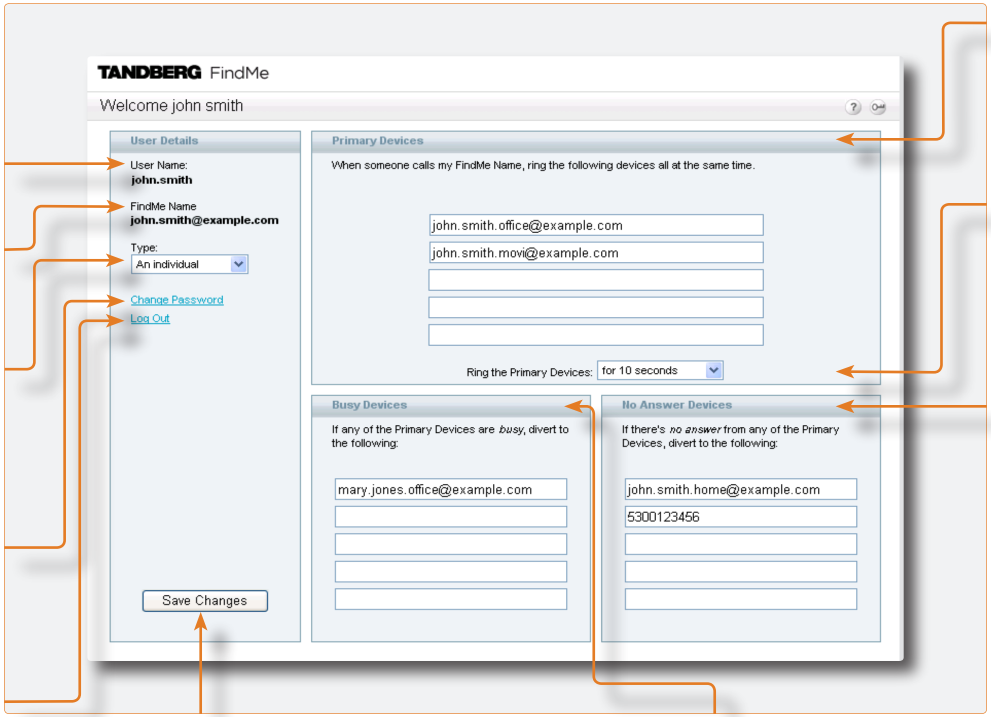
Username
The username for this FindMe account.

FindMe name
The FindMe name being configured.

Type
Select whether this FindMe name is to apply to an individual or a group of people. This will affect how calls are diverted to the Busy devices.

Change Password
Click here to change the password used to access your FindMe account. You will be taken to a new page where you can enter the new password.

Log Out
Click here to exit the FindMe account configuration page.



Primary Devices
List the all the device(s) that will ring when your FindMe name is first dialled.

If more than one device is listed here, they will all ring at the same time.

Ring the primary devices
Select the amount of time in seconds you wish the devices in the Primary list to ring before the call is diverted. Alternatively, you can specify that the devices will ring until the caller hangs up.

No Answer Devices
List all the device(s) that will ring if none of the devices in the Primary list are answered within the specified time.

If no devices are listed here, the caller will receive a "no answer" response if none of the Primary devices are answered.

If you have selected a Timeout period of ring until caller hangs up, you will not be able to list any devices here.

Save Changes
Click here to update your FindMe account with any changes.

Busy Devices
For an individual, list all the device(s) that will ring immediately if any of the devices in the Primary list are busy.

For a group of people, list all the device(s) that will ring immediately if all of the devices in the Primary list are busy. (If some of the devices in the Primary list are busy, the rest will continue to ring for the specified time before the call will divert to the devices listed here.)

If no devices are listed in this section, the caller will get a busy response if any/all of the Primary devices are busy.

Ensure that none of the Primary devices are set to Autoanswer. If they are, the system will consider the call to have been answered when Autoanswer is initiated, and so it will not divert the call to any other devices.

Adding a device to a list
You can have up to five devices in each list. To add a device to any of the lists, enter one of the following in any of the available fields:

- for video endpoints: enter any URL or alias with which the device is registered.
- for 3G mobile phones: to route video to your mobile phone, you must have a 3G gateway - enter the gateway's prefix followed by the mobile phone number. To route voice only, enter the mobile phone number along with any prefixes required by your dial plan for external calls.
- for telephones: enter the extension number (for internal calls) or telephone number, along with any necessary prefixes.

Removing a device
To remove a device from a list, simply delete the text from the relevant field.

Alias Searching and Transforming

Overview of Searches and Transforms

About Searches

One of the VCS's functions is to process incoming requests to search for a particular alias. These search requests are received from

- locally registered endpoints
- Alternates
- neighbor zones, including traversal clients and traversal servers.

Regardless of the origin of the request, the VCS will always follow a set sequence of steps when searching for an alias, stopping as soon as the alias has been found or moving on to the next step if it has not. The steps are as follows:

1. The VCS searches its local zone to see if the alias belongs to any endpoints registered directly to it.
2. The VCS forwards the search request to all its Alternates.
3. The VCS forwards the search request to its neighboring zones. Which zones are searched, and in what order, depends on the zone search settings for that zone.

About Transforms

The VCS allows you to transform the alias in a search request if it matches certain criteria. This transformation can be applied to the alias at two points in the search process:

- as soon as it is received and before it is searched for locally
- before sending a search request out to neighboring zones.

You can transform the alias by removing or replacing its prefix, suffix, or the entire string, and by the use of regular expressions.

All Alternates should be configured identically, including any local zone transforms. However, this means that an alias that was not found locally would be transformed twice - once before the local zone was searched and again after being sent to the Alternate, before the Alternate searched its own local zone. To prevent this, a VCS is able to determine whether a search request has come from one of its Alternates and if so will not transform the alias before searching for it locally.

Transforming an Alias Before Searching Locally

About Local Alias Transforms

The local alias transform function allows you to modify the alias in an incoming search request before conducting the search locally. It applies to all incoming search requests from locally registered endpoints and from neighboring VCSs. It does not apply to search requests from Alternates.

Each local alias transform defines a string against which an alias is compared, and the changes to make to the alias if it matches that string.

Local zone alias transforms will be applied prior to any possible CPL modification and Zone transforms. These alias transforms will not have any effect on aliases presented in GRQ or RRQ messages.

Local Alias Transform Process

Up to 100 local alias transforms can be configured. Each transform must have a unique priority number between 1 and 65534.

Every incoming alias is compared with each transform in order of priority, starting with that closest to 1. If and when a match is made, the transform is applied to the alias and no further checks or transformations of the new alias will take place. The new alias is then searched for locally.

If you add a new transform that has the same priority as an existing transform, all transforms with a lower priority will be moved down the list, and the new transform will be added with the specified priority. However, if there are not enough slots left to move all the priorities down, then you will get an error message.

If the Transformed Alias is Not Found Locally

If the new alias is not found locally, the search is expanded first to Alternates and then to neighbors.

- When an Alternate is queried, it will identify that the request has come from one of its own Alternates and will search for the transformed alias locally without applying any further transforms.
- When neighbors are queried, you can specify further transforms to be applied prior to sending out the search request. The neighbor's configuration may also be such that it will transform the alias before searching for it locally.

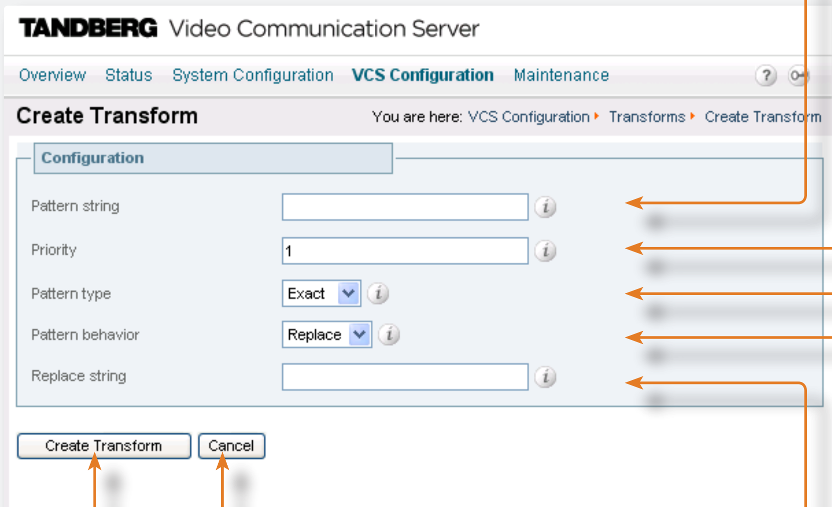
Alias Searching and Transforming

Transforming an Alias Before Searching Locally: Configuration

Configuring Local Alias Transforms

To configure local alias transforms:

- *VCS Configuration > Transforms*.
  You will be taken to the Transforms page.
  Click New.
  You will be taken to the Create Transform page.
- `xConfiguration Transform [1..100]`.



Pattern string

Specifies the pattern against which the alias is compared.

Priority

Assigns a priority to this transform. Transforms are applied in order of priority, and the priority must be unique for each transform.

Pattern type

Determines the way in which the string must match the alias. Options are:

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Pattern behavior

Determines how the matched part of the alias will be modified. Options are:

Strip: the matching prefix or suffix will be removed from the alias.

Replace: the matching part of the alias will be substituted with the text in the Replace String.

Local transforms support the use of Regular Expressions. See the Appendix Regular Expression Reference for more information.

Create Transform

Click here to save the transform and return to the Transforms page.

Cancel

Click here to return to the Transforms page without adding the new transform.

Replace string

(applies only if Pattern Behavior is set to Replace)

Specifies the string to be used as a substitution for the part of the alias that matched the pattern.

Alias Searching and Transforming

Zone Searching and Transforming

About Zone Searching

The VCS allows you to filter the search requests sent to each zone, and prioritize the order in which zones are searched. This allows you to reduce the potential number of search requests sent out, and speed up the search process.

The VCS uses the concept of zone “matches” when filtering search requests to zones. Each zone has up to five configurable “matches” available to it. Each match is assigned a Mode and Priority (described below). The combination of the two determines if and when that zone will be queried.

Mode

The match Mode allows you to specify whether and how you will filter requests to the zone. Alternatively, you can use this mode to prevent search requests from ever being sent to the zone.

The Mode options are:

AlwaysMatch: always query the zone

PatternMatch: only query the zone if the alias being searched for matches a specified pattern

Disabled: never query the zone (this mode does not need a corresponding Priority option).

Priority

The match Priority allows you to specify when in the search process that zone will be queried. Search requests are sent to all zones with a Priority 1 match first, followed by all zones with Priority 2 matches, and so on.

It is possible for the same priority to be given to more than one match, either in the same zone or in different zones. In this case, all zones with that match priority will be queried at the same time.

About Zone Transforms

The VCS allows you to change the alias being searched for before a search request is sent out to a particular zone. This feature uses the PatternMatch mode of the zone search function.

To set up a zone transform, you must:

- configure the zone with a Mode of PatternMatch
- specify the pattern that the alias to be transformed must match
- specify the way in which the alias will be transformed.

All searches sent to that zone that match the specified pattern will then be transformed and the zone will be queried using the new alias.

Each zone has up to five configurable matches. This means that you can specify up to five different transforms for each zone. This could be:

- one alias transformed five different ways
- five aliases each transformed individually
- a combination of both.

Using Zone Searches and Transforms Together

The zone searching feature and the zone transforms feature both make use of the PatternMatch mode. You can use these two features together or separately.

The remainder of this section:

- describes the zone search and transform process
- explains how to configure zone searches and transforms
- gives some examples of how zone searches and transforms could be used together.

Zone Search and Transform Process

Zones are queried when an alias has not been found locally. The search and transform process is as follows:

1. The VCS looks at all matches for all zones to find all those with either:
   - a Mode of AlwaysMatch, or
   - a Mode of PatternMatch and a Pattern String that matches the alias being searched for.
2. These matches are listed in order of the Priority that has been assigned to them.
3. If there are any duplicates in the list, the entry with the lower Priority is removed. (This applies to a zone with the same pattern string and the same transform but different priorities.)
4. If there is a zone which has an AlwaysMatch as well as a PatternMatch with no transforms, the PatternMatch is removed from the list.
5. All zones with a Priority 1 match on the list are queried. For AlwaysMatch matches, the query will use the original alias; for PatternMatch matches the query will use the alias specified by the transform rules.
6. If the alias is found, the call will be forwarded to that zone. If the alias is found by more than one zone, the call will be forwarded to the zone that responded first.
7. If the alias is not found, all zones with a Priority 2 match are queried as per steps 5 and 6.
8. The process is repeated until either:
   - the alias is found, or
   - all zones with a match that meets the specified criteria have been queried.

Zone searching and alias transforming: configuration

Configuring Zone Searches and Transforms

To configure when a zone will be searched and any transforms that will be applied before the search request is sent:

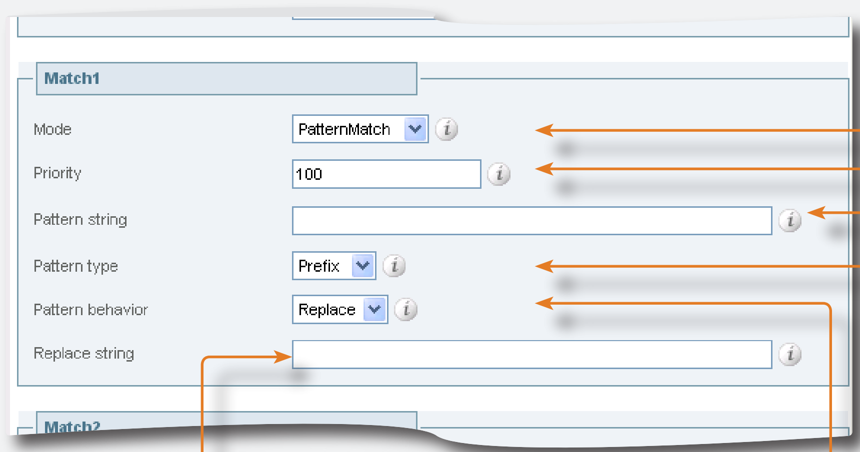
- *VCS Configuration > Zones*.
  You will be taken to the Zones page.
  Click on the zone you wish to configure.
  You will be taken to the Edit Zone page.
  Scroll down until you get to the Match1 section.
- `xConfiguration Zones Zone [1..200] Match [1..5]`

You can configure up to five different Matches (i.e. search/transform combinations) for each zone.

Default Settings

When a new zone is created, by default Match1 will be set to AlwaysMatch with a Priority of 100. All remaining matches will be set to Disabled. This means that the zone will be queried for the original alias, with no transforms applied.

Zone transforms support the use of Regular Expressions. See the Appendix [Regular Expression Reference](#) for more information.



Replace string

(Applies only if the Mode is PatternMatch and Pattern Behavior is Replace.)

Specifies the string to be used as a substitution for the part of the alias that matched the pattern.

Pattern behavior

(Applies only if the Mode is PatternMatch.)

Determines if and how the matched part of the alias will be modified. Options are:

Leave: the alias will not be modified.

Strip: the matching prefix or suffix will be removed from the alias.

Replace: the matching part of the alias will be substituted with the text in the Replace String.

Mode

Determines if and when a query will be sent to this zone. Options are:

AlwaysMatch: the zone will always be queried.

PatternMatch: the zone will only be queried if the alias queried for matches the specified Pattern String.

Disabled: the zone will never be queried.

Priority

Determines the order in which the zone will be sent a search request. Zones with priority 1 matches are searched first, followed by priority 2, and so on. More than one match can be assigned the same priority; in this case the matches will be queried simultaneously.

Pattern string

(Applies only if the Mode is PatternMatch.)

Specifies the pattern against which the alias is compared.

Pattern type

(Applies only if the Mode is PatternMatch.)

Determines the way in which the string must match the alias. Options are:

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Examples

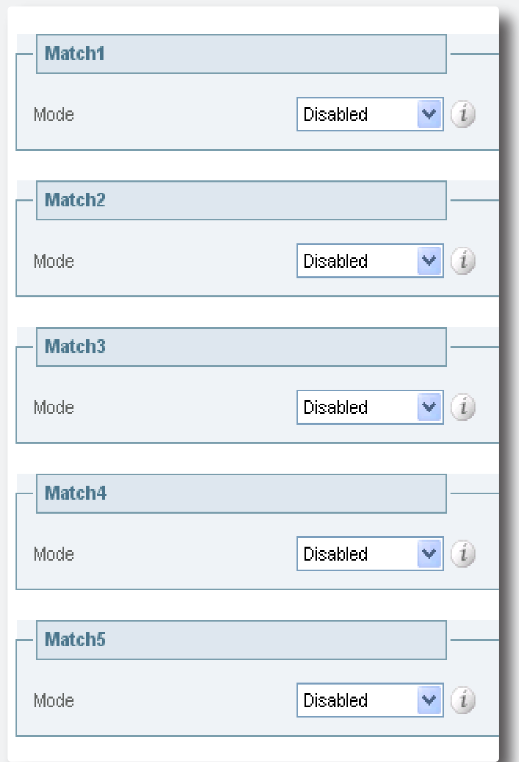
Combining Match Types and Priorities

By using both AlwaysMatch and PatternMatch matches in the same zone, and applying the same or different priorities to each match, you will have a great deal of flexibility in determining if and when the zone will be queried and whether any transforms will be applied. Some example configurations are given here.

The AlwaysMatch mode does not support alias transforms. Should you wish to always query a zone using a different alias to that received, you will need to use a mode of PatternMatch in combination with a regular expression.

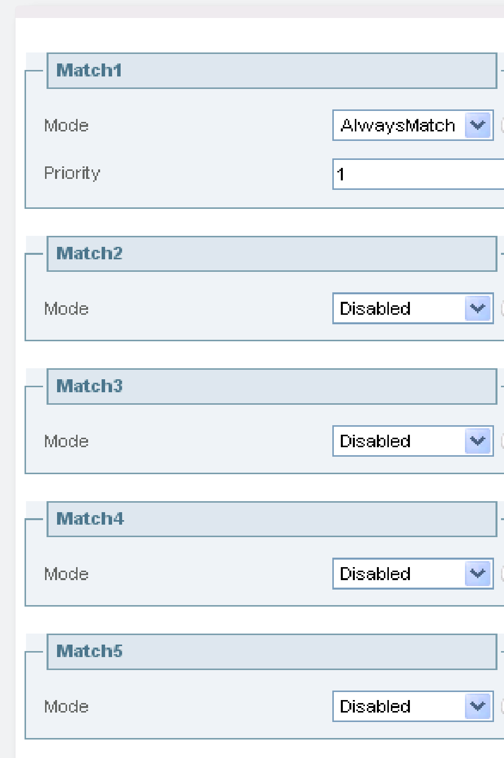
Never Query a Zone

To configure the zone so that it is never sent an alias search request, set all 5 matches to a Mode of Disabled.



Always Query a Zone, Never Apply Transforms

To configure the zone so that it is always sent search requests using the original alias, set the following:



Examples

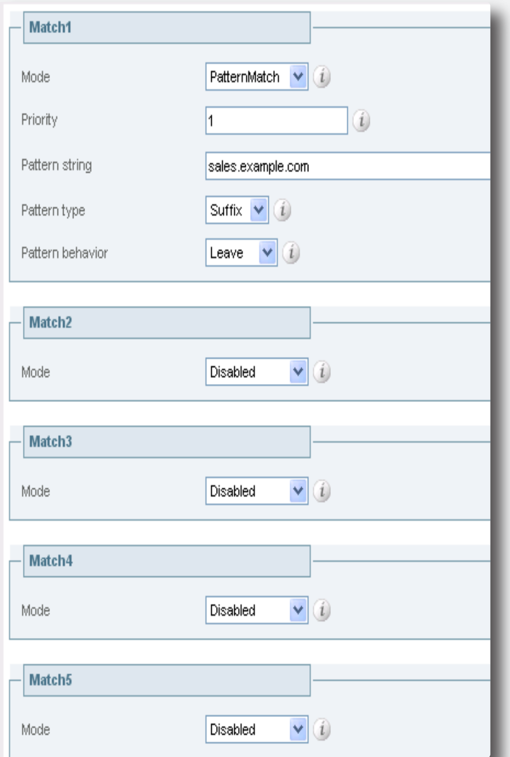
Filter Queries to a Zone Without Transforming

It is possible to filter the search requests sent to a zone so that it is only queried for aliases that match a particular criteria.

For example, all endpoints in your regional sales office are registered to their local VCS with a suffix of @sales.example.com.

In this situation, it makes sense for your head office VCS to query the sales office VCS only when it receives a search request for an alias with a suffix of @sales.example.com. Sending any other search requests to this particular VCS would take up resources unnecessarily.

To achieve this, on your local VCS create and configure the zone representing the sales office VCS as shown:



Changing the Prefix or Suffix Before Querying

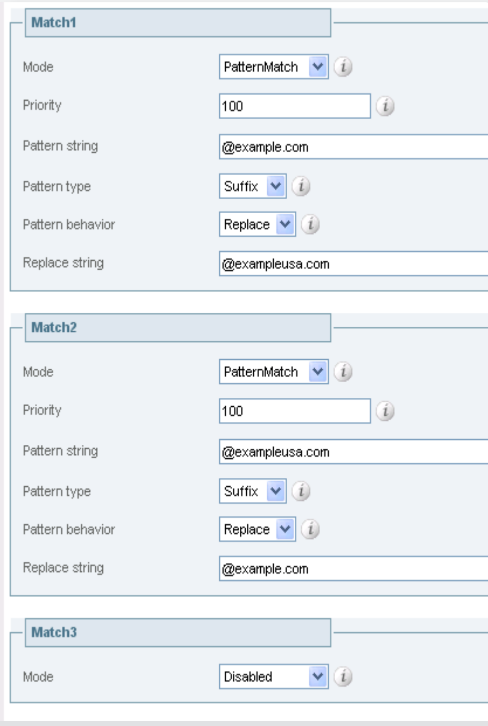
It is possible to direct an incoming search request to a different alias by replacing either the prefix or the suffix of the alias with a new string.

For example, your know that endpoints in a neighbor zone are registered to their local VCS with aliases in two different formats:

- user@example.com and
- user@exampleusa.com.

You want to ensure that if anyone dials user@exampleusa.com from one of your locally registered endpoints, they will be able to find that person at user@example.com, and vice versa.

To achieve this, on your local VCS configure the zone representing the neighbor VCS as shown:



Alias Searching and Transforming

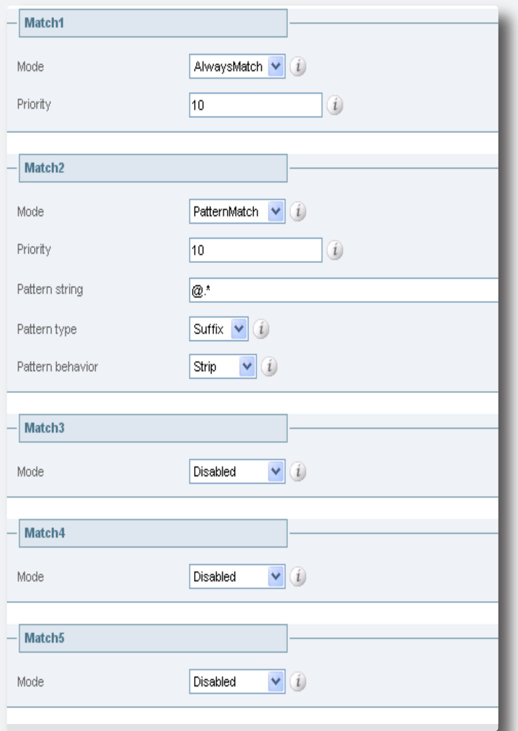
Examples

Query a Zone for Both Original and Transformed Alias

You may wish to query a zone for the original alias at the same time as you query it for a transformed alias. To do this, configure one match with a mode of AlwaysMatch, and a second match with a mode of PatternMatch along with details of the transform to be applied. Both matches must be given the same Priority level.

For example, you may wish to query a neighbor zone for both a full URI and just the name (i.e. the URI with the domain removed).

To achieve this, on your local VCS configure the zone representing the neighbor VCS as shown:

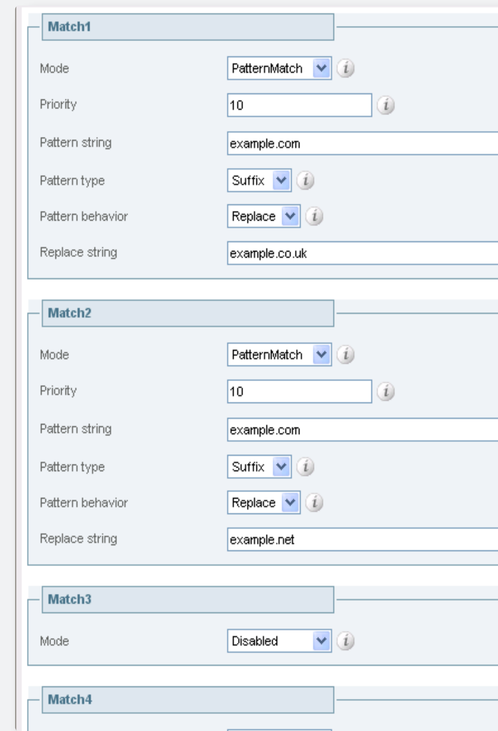


Query a Zone for Two or More Transformed Aliases

Zones are queried in order of priority of the matches configured within them.

It is possible to configure a single zone with up to five PatternMatch matches, each with the same Priority and with an identical Pattern String to be matched, but each with a different replacement pattern. In this situation, the VCS will query that zone for each of the new aliases simultaneously. (Any duplicate aliases produced by the transforms will be removed prior to the search requests being sent out.)

If any of the new aliases are found by that zone, the call will be forwarded to the zone. It is then up to the controlling system to determine the alias to which the call will be forwarded.



URI Dialing Overview

About URI Dialing

A URI address typically takes the form name@example.com, where name is the alias and example.com is the domain.

URI dialing makes use of DNS to enable endpoints registered with different systems to locate and call each other. With URI dialing, it is possible to find an endpoint by using DNS to locate the domain in the URI address and then query that domain for the alias.

Without URI dialing, you would need to neighbor all the systems to each other in order for one system to be able to locate an endpoint registered to another system. This does not scale well as the number of systems grows. It is also inconvenient for making one-off calls to endpoints registered with previously unknown systems.

Endpoints must register with the VCS using a URI address in order to be reachable using URI dialing.

URI Resolution Process via DNS

When a system is attempting to locate a destination URI address using the DNS system, the general process is as follows:

1. The system will send a query (via its DNS server) for a SRV record for the domain in the URL. If available, this SRV record will return information about the authoritative gatekeeper (H.323) or proxy (SIP) for that domain (e.g. its FQDN and listening port).
   The system will then send out another query for an A/AAAA record for the FQDN returned in the SRV record. If available, this will return the actual IP address of the gatekeeper/proxy. Once its IP address has been discovered, the system will query that gatekeeper/proxy for the URI.
2. If a relevant SRV record cannot be located, the system will fall back to looking for an A or AAAA record for the domain in the URL. If such a record is found, the call will be routed to that IP address.

Enabling URI Dialing via the VCS

URI dialing is enabled separately for outgoing and incoming calls.

Outgoing Calls

To enable endpoints registered to your VCS to place calls directly using URI dialing, you must:

- configure at least one DNS zone, and
- configure at least one DNS Server.

This is described in the section Configuring URI dialing for outgoing calls.

Incoming Calls

To enable endpoints registered to your VCS to receive calls directly using URI dialing, you must:

- ensure all endpoints are registered with a URI address
- configure appropriate DNS records, depending on the protocols and transport types you wish to use.

This is described in the section Configuring URI dialing for Incoming calls.

Firewall Traversal Calls

To configure your system so that you can place and receive calls using URI dialing through a firewall, see the section URI Dialing and firewall traversal.

If a DNS zone and/or a DNS server have not been configured on the local VCS, calls made using URI dialing could still be placed if the local VCS is neighbored with another VCS that has been appropriately configured. Any URI dialed calls will go via the neighbor. This configuration is useful if you want all URI dialing to be made via one particular system, e.g. a VCS Border Controller.

URI Dialing for Outgoing Calls

Process

When a user places a call using URI dialing, they will typically dial an address in the form name@example.com from their endpoint. Below is the process that is followed when a URI address is dialed from an endpoint registered with your VCS:

1. The VCS will check its own list of registrations, and those of its Alternates, to see if the address is registered locally.
2. If the address is not registered locally, the VCS will check all its zones to see if any of them are configured with either:
   - an AlwaysMatch, or
   - a PatternMatch with a pattern that matches the URI address.

   These zones will then be queried in priority order for the URI.
3. If one or more of the zones that contain a match are neighbor zones, the neighbor will be queried for the URI. If the neighbor supports URI dialing, it may route the call itself.
4. If one or more of the zones that contain a match are DNS zones, this will trigger the VCS to attempt to locate the endpoint through a DNS lookup. It does this by querying the DNS server configured on the VCS for the location of the domain as per the DNS resolution process.
5. If the domain part of the URI address was resolved successfully using an H.323 Location SRV record (i.e. for `_h323ls)` then the address returned is queried via an LRQ for the full URI address.
6. If the domain part of the URI address was resolved using an H.323 Call SRV record (i.e. for `_h323cs)` or an `A/AAAA` record lookup then the call is routed directly to the IP address returned in that record. An exception to this is where the original dial string has a port specified (e.g. **`user@example.com:1720`**) in which case the address returned is queried via an LRQ for the full URI address.
7. If the domain part of the URI address was resolved successfully using a SIP SRV record (i.e. for `_sip)` then the request is forwarded to the address returned.

Configuring Matches for DNS Zones

If you wish locally registered endpoints to be able to place URI calls via the VCS, then at a minimum you should configure a DNS zone with a match that has a Mode of AlwaysMatch. This will result in DNS always being queried, but will mean it is queried for all aliases, not just URI addresses.

To filter the queries sent to the DNS server:

- configure a DNS zone with a match that has a Mode of PatternMatch
- use the Pattern string and Pattern type fields to define the aliases that will trigger a DNS query.

For example, a match with a Pattern string of **`*@*`** and a Pattern type of Regex will mean that DNS is only queried for aliases in the form of typical URI addresses.

To set up further filters, configure the remaining matches in the same DNS zone. You don't need to create new DNS zones unless you want to configure more than the maximum of 5 matches.

You should create separate DNS zones if you want to filter based on the protocol (SIP or H.323) or hop count to be used.

URI Dialing for Outgoing Calls

Adding and Configuring DNS Zones

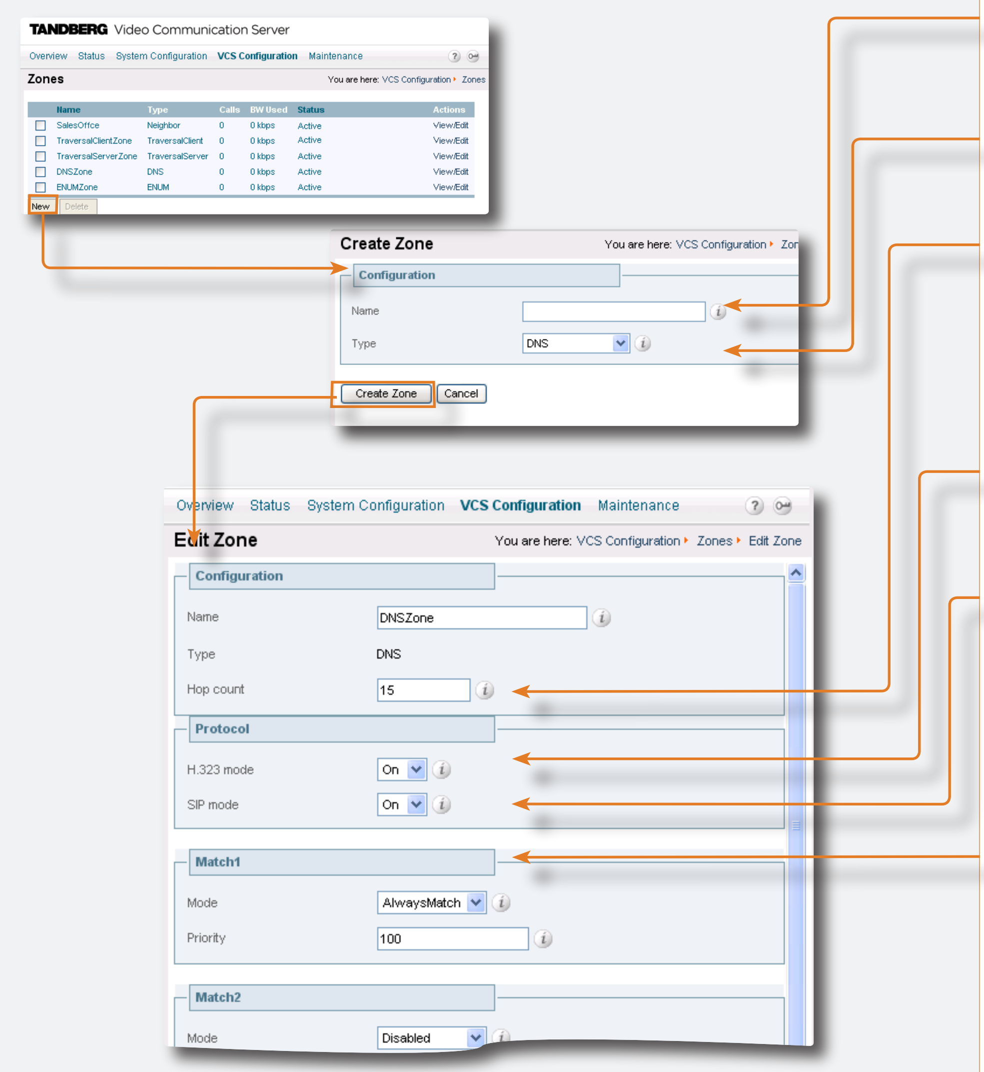
In order for locally registered endpoints to use URI dialing through the VCS, you must configure at least one DNS zone. To do this:

- *VCS Configuration > Zones*.
  You will be taken to the Zones page.
  Click New.
  You will be taken to the Create Zone page.
  Enter a Name for the zone and select a Type of DNS.
  Click Create Zone.
  You will be taken to the Edit Zone page.
- xCommand ZoneAdd
- xConfiguration Zones Zone [1..200]

Normal zone pattern matching and prioritization rules will apply to DNS zones.

When dialing by URI, the hop count used is that configured for the DNS zone that matches the URI address.

If there is no DNS zone configured that matches the URI address, then the query may be forwarded to a neighbor. In this case, the hop count used will be that configured for the neighbor zone.



Name

Assigns a name to this zone.

Type

For DNS zones, this will be DNS.

Hop count

Specifies the hop count to be used when sending an alias search request to this zone. If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.

H.323 mode

Determines whether or not H.323 calls will be allowed to this zone.

SIP mode

Determines whether or not SIP calls will be allowed to this zone.

Match1 - Match5

These sections allow you to specify any filtering criteria you wish to apply to this zone.

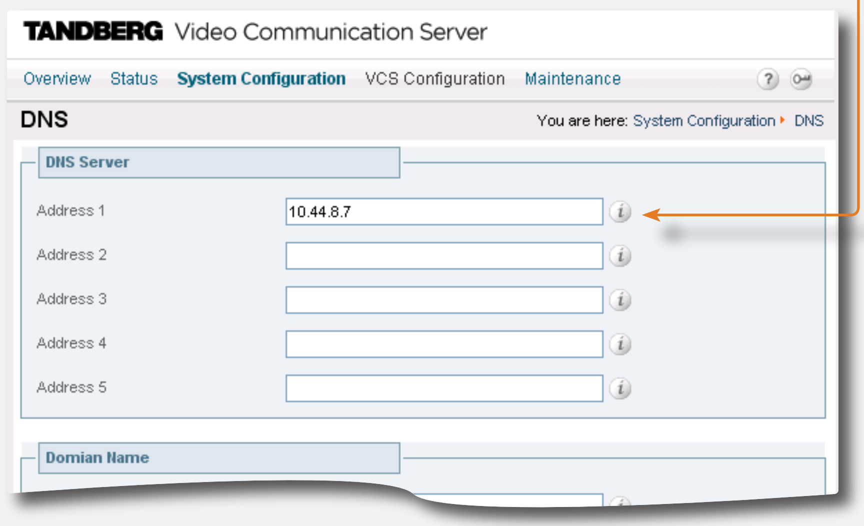
See Configuring Matches for DNS zones for full information on how the Match options can be used.

URI Dialing for Outgoing Calls

Configuring DNS Servers

To configure the DNS servers to be used by the VCS when querying DNS:

- *System Configuration > DNS*.
  You will be taken to the DNS page.
- xConfiguration IP DNS Server



Address 1 to Address 5

Enter the IP address(es) of up to 5 DNS servers that the VCS will query when attempting to locate a domain.

In order for endpoints registered to the VCS to make outgoing calls using URI dialing, you must configure at least one DNS server for the VCS to query. For resilience, you can specify up to five DNS servers.

The DNS server(s) configured here are used as part of both the ENUM dialing and URI dialing processes.

URI Dialing for Incoming Calls

Types of DNS Records Required

The ability of the VCS to receive incoming calls made via URI dialing relies on the presence of DNS records for each domain the VCS is hosting.

These records can be of various types including:

- A records, which provide the IPv4 address of the VCS
- AAAA records, which provide the IPv6 address of the VCS
- Service (SRV) records, which specify the FQDN of the VCS and the port on it to be queried for a particular protocol and transport type.

As a preference, SRV records should be used, and you should provide an SRV record for each combination of domain hosted and protocol and transport type enabled on the VCS.

Process

When an incoming call has been placed using URI dialing, the VCS will have been located by the calling system via one of the DNS record lookups described above. It will receive the request containing the dialled URI in the form user@xample.com. The VCS will then check its local registrations and FindMe names and if any are an exact match, the call will be routed to the appropriate device(s).

In order for locally registered endpoints to be reached using URI dialing, they must register using a full URI. This applies to both SIP and H.323 endpoints. If endpoints do not register using a full URI, they will be discoverable only by the VCS to which they are registered, and any neighbor VCSs.

Several mechanisms could have been used to locate the VCS. You may wish to enable calls placed to user@VCS_IP_address to be routed to an existing registration for user@example.com. In this case you would configure a Local Zone Transform that would strip the IP address of the VCS from the incoming URI and replace it with the domain name of example.com.

SRV Record Format

The format of SRV records is defined by RFC 2782 [3] as:

`_Service._Proto.Name TTL Class SRV Priority Weight Port Target`

For the VCS, these will be as follows:

- `_Service` and `_Proto` will be different for H.323 and SIP, and will depend on the protocol and transport type being used.
- `Name` is the domain in the URI that the VCS is hosting (e.g. example.com)
- `Port` is the port on the VCS that has been configured to listen for that particular service and protocol combination
- `Target` is the FQDN of the VCS.

Configuring H.323 SRV Records

Annex O of H.323 [15] defines the procedures for using DNS to locate gatekeepers and endpoints and for resolving H.323 URL aliases. It also defines parameters for use with the H.323 URL.

The VCS supports two types of SRV record as defined by this Annex. These are Location and Call, with `_Service` set to `_h323ls` and `_h323cs` respectively.

If you wish the VCS to be contactable via H.323 URI dialing, you should provide at least a Location SRV record, as it provides the most flexibility and the simplest configuration.

Location SRV Records

For each domain hosted by the VCS, you should configure a Location SRV record as follows:

- `_Service` is `_h323ls`
- `_Proto` is `_udp`
- `Port` is the port number that has been configured via *VCS Configuration > Protocols > H.323* as the Registration UDP port.

Call SRV Records

Call SRV records (and A/AAAA records) are intended primarily for use by endpoints which cannot participate in a location transaction, exchanging LRQ and LCF. The configuration of a Call SRV record should be as follows:

- `_Service` is `_h323cs`
- `_Proto` is `_tcp`
- `Port` is the port number that has been configured via *VCS Configuration > Protocols > H.323* as the Call signaling TCP port.

Configuring SIP SRV Records

RFC 3263 [16] describes the DNS procedures used to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact.

If you wish the VCS to be contactable via SIP URI dialing, you should configure an SRV record for each SIP transport protocol enabled on the VCS (i.e. UDP, TCP or TLS) as follows:

- `_Service` is `_sip`
- `_Proto` is one of `_udp`, `_tcp`, or `_tls`
- `Port` is the port number that has been configured via *VCS Configuration > Protocols > SIP* as the port for that particular transport protocol.

URI Dialing

URI Dialing for Incoming Calls

Example DNS Record Configuration

A company with the domain name example.com wants to enable incoming H.323 and SIP calls using URI addresses in the format user@example.com. The VCS hosting the domain has the FQDN vcs.example.com.

Their DNS records would typically be as follows:

- SRV record for `_h323ls._udp.example.com` returns `vcs.example.com`
- SRV record for `_h323cs._tcp.example.com` returns `vcs.example.com`
- SRV record for `_sip._udp.example.com` returns `vcs.example.com`
- SRV record for `_sip._tcp.example.com` returns `vcs.example.com`
- SRV record for `_sip._tls.example.com` returns `vcs.example.com`
- A record for `vcs.example.com` returns the IPv4 address of the VCS
- AAAA record for `vcs.example.com` returns the IPv6 address of the VCS

How you add the DNS records depends on the type of DNS server you are using. Instructions for setting up two common DNS servers are given in the Appendix DNS Configuration.

URI Dialing and Firewall Traversal

Recommended Configuration

If URI dialing is being used in conjunction with firewall traversal, DNS zones and DNS Servers should be configured on the VCS Border Controller and any VCSs on the public network only. VCSs behind the firewall should not have any DNS zones or servers configured. This will ensure that any outgoing URI calls made by endpoints registered with the VCS will be routed through the VCS Border Controller.

In addition, the DNS records should be configured with the address of the VCS Border Controller as the authoritative gatekeeper/proxy for the enterprise (see the Appendix DNS Configuration). This ensures that incoming calls placed using URI dialing enter the enterprise through the VCS Border Controller, allowing successful traversal of the firewall.

ENUM Dialing

ENUM Dialing Overview

About ENUM Dialing

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias.

The E.164 number is converted into a URI by the DNS system, and the rules for URI dialing are then followed to place the call.

The ENUM dialing facility allows you to retain the flexibility of URI dialing whilst having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing via a numeric keypad.

The VCS supports outward ENUM dialing by allowing you to configure ENUM zones on the VCS. When an ENUM zone is queried, this triggers the VCS to transform the E.164 number that was dialed into an ENUM domain which is then queried via DNS.

Note however that ENUM dialing relies on the presence of relevant DNS NAPTR records for the ENUM domain being queried. These are the responsibility of the administrator of that domain.

ENUM Process

When a system is attempting dial a destination endpoint using ENUM, the general process is as follows:

1. The user dials the E.164 number from their endpoint.
2. The system converts the E.164 number into an ENUM domain as follows:
   a. the digits are reversed and separated by a dot
   b. the name of the domain that is hosting the NAPTR records for that E.164 number is added as a suffix.
3. DNS is then queried for the resulting ENUM domain.
4. If a NAPTR record exists for that ENUM domain, this will advise how the number should be converted into one (or possibly more) H.323/SIP URIs.
5. The system then sends out another DNS query for that URI. From this point the process for URI Dialing is followed.

Enabling ENUM Dialing

ENUM dialing is enabled separately for incoming and outgoing calls.

Outgoing Calls

To allow locally registered endpoints to dial out to other endpoints using ENUM, you must

- configure at least one ENUM zone, and
- configure at least one DNS Server.

This is described in the section Configuring ENUM Dialing for outgoing calls.

Incoming Calls

To enable endpoints in your enterprise to receive incoming calls from other endpoints via ENUM dialing, you must configure a DNS NAPTR record mapping your endpoints' E.164 numbers to their SIP/H.323 URIs. See the section Configuring ENUM dialing for incoming calls for instructions on how to do this.

If an ENUM zone and/or a DNS server have not been configured on the local VCS, calls made using ENUM dialing could still be placed if the local VCS is neighbored with another VCS that has been appropriately configured. Any ENUM dialed calls will go via the neighbor. This configuration is useful if you want all ENUM dialing from your enterprise to be configured on one particular system.

ENUM Dialing for Outgoing Calls

Prerequisites

In order for a local endpoint to be able to dial a remote endpoint using ENUM via your VCS, the following three conditions must be met:

1. There must be a NAPTR record available in DNS that maps the remote endpoint's E.164 number to its URI. It is the responsibility of the administrator of the remote enterprise to provide this record, and they will only make it available if they wish the endpoints in their enterprise to be contactable via ENUM dialing.
2. You must configure an ENUM zone on your local VCS. This ENUM zone must have a DNS Suffix that is the same as the domain where the NAPTR record for the remote endpoint is held.
3. You must configure your local VCS with the address of at least one DNS server that it can query for the NAPTR record (and if necessary any resulting URI).

Process

Below is the process that is followed when an ENUM (E.164) number is dialed from an endpoint registered with your VCS:

1. The user dials the E.164 number from their endpoint.
2. The VCS initiates a search for the E.164 number as dialed. It follows the usual alias search process, first applying any local zone transforms, then searching local and Alternate registrations and FindMe names for the E.164 number.
3. If the E.164 number is not found locally, the VCS will check all its zones to see if any of them are configured with either:
   - an AlwaysMatch, or
   - a PatternMatch with pattern that matches the E.164 number.

   These zones will then be queried in priority order.
4. If one or more of the zones that contain a match is a neighbor zone, the neighbor will be queried for the E.164 number. If the neighbor supports ENUM dialing, it may route the call itself.
5. If one or more of the zones that contain a match is an ENUM zone, this will trigger the VCS to attempt to locate the endpoint through ENUM. As and when each ENUM zone configured on the VCS is queried, the E.164 number is transformed into an ENUM domain as follows:
   a. the digits are reversed and separated by a dot
   b. the DNS Suffix configured for that ENUM zone is appended.
6. DNS is then queried for the resulting ENUM domain.
7. If the DNS server finds at that ENUM domain a NAPTR record that matches the transformed E.164 number (i.e., after it has been reversed and separated by a dot), it returns the associated URI to the VCS.
8. The VCS then initiates a new search for that URI (maintaining the existing hop count). The VCS starts at the beginning of the search process (i.e. applying any local zone transforms, then searching locally, then searching zones). From this point, as it is now searching for a SIP/H.323 URI, the process for URI Dialing is followed.

Example

In this example, we wish to call Fred at Example Corp. Fred's endpoint is actually registered with the URI fred@example.com, but to make it easier to contact him his system administrator has configured a DNS NAPTR record mapping this alias to his E.164 number: +44 118 123 456.

We know that the NAPTR record for example.com uses the DNS domain of e164.arpa.

1. We create an ENUM zone on our local VCS with a DNS suffix of `e164.arpa`.
2. We configure this zone with a pattern match mode of AlwaysMatch, so that ENUM will always be queried regardless of the format of the alias being searched for.
3. We dial `44 118 123 456` from our endpoint.
4. The VCS initiates a search for a registration of 44 118 123 456. Because the ENUM zone we have configured has a match mode of AlwaysMatch, it is queried at the same time as any other zones with a matching priority.
5. Because the zone being queried is an ENUM zone, the VCS is automatically triggered to transform the number into an ENUM domain as follows:
   a. the digits are reversed and separated by a dot: `6.5.4.3.2.1.8.1.1.4.4`
   b. the DNS Suffix configured for this ENUM zone, `e164.arpa`, is appended.

   This results in a transformed domain of `6.5.4.3.2.1.8.1.1.4.4.e164.arpa`.
6. DNS is then queried for that ENUM domain.
7. The DNS server finds the domain and returns the information in the associated NAPTR record. This tells the VCS that the E.164 number we have dialed is mapped to the SIP URI of fred@example.com.
8. The VCS then starts another search, this time for fred@example.com. From this point the process for URI Dialing is followed, and results in the call being forwarded to Fred's endpoint.

ENUM Dialing for Outgoing Calls

Configuring Matches for ENUM Zones

If you wish locally registered endpoints to be able to make ENUM calls via the VCS, then at a minimum you should configure an ENUM zone with:

- a match that has a Mode of AlwaysMatch
- a DNS suffix of e164.arpa (the domain specified by the ENUM standard).

This will result in DNS always being queried for all aliases, not just ENUMs. It will also mean that ENUM dialing will only be successful if the enterprise being dialed uses the e164.arpa domain.

To ensure successful ENUM dialing, you must configure an ENUM zone for each domain that holds NAPTR records for endpoints that callers in your enterprise might wish to dial.

Once these ENUM zones have been created, you can filter the queries that are sent to each as follows:

- configure a match that has a Mode of PatternMatch
- use the Pattern string and Pattern type fields to define the aliases that will trigger an ENUM lookup.

Example

For example, you want to enable ENUM dialing from your network to a remote office in the UK where the endpoints' E.164 numbers start with `44`. You would configure an ENUM zone on your VCS that has a Match configured as follows:

- Mode of PatternMatch
- Pattern string of `44`
- Pattern type of Prefix.

This will result in an ENUM query being sent to that zone only when someone dials a number starting with `44`.

Configuring Transforms for ENUM Zones

You can configure transforms for ENUM zones in the same way as any other zones (see Zone Searches and Transforms for full information).

If there are any transforms configured for an ENUM zone, these will be applied prior to the number being converted to an ENUM domain.

Example

For example, you want to enable ENUM dialing from your network to endpoints at a remote site using a prefix of `8` followed by the last 4 digits of the remote endpoints' E.164 number. You would configure an ENUM zone on your VCS that has a Match configured as follows:

- Mode of PatternMatch
- Pattern string of `8(\d{4})`
- Pattern type of Regex
- Pattern behavior of Replace
- Replace string of `44123123(\1)`

With this configuration, it will be the resulting string (i.e. `44123123xxxx`) that will then be converted into an ENUM domain and queried for via DNS.

To verify that you have configured your outward ENUM dialing correctly, use the `xCommand Locate` command to try and resolve an E.164 alias.

ENUM Dialing for Outgoing Calls

Configuring ENUM Zones

In order for locally registered endpoints to use ENUM dialing, you must configure an ENUM zone for each ENUM service used by remote endpoints. To do this:

- *VCS Configuration > Zones*.
  You will be taken to the Zones page.

  Click New.
  You will be taken to the Create Zone page.

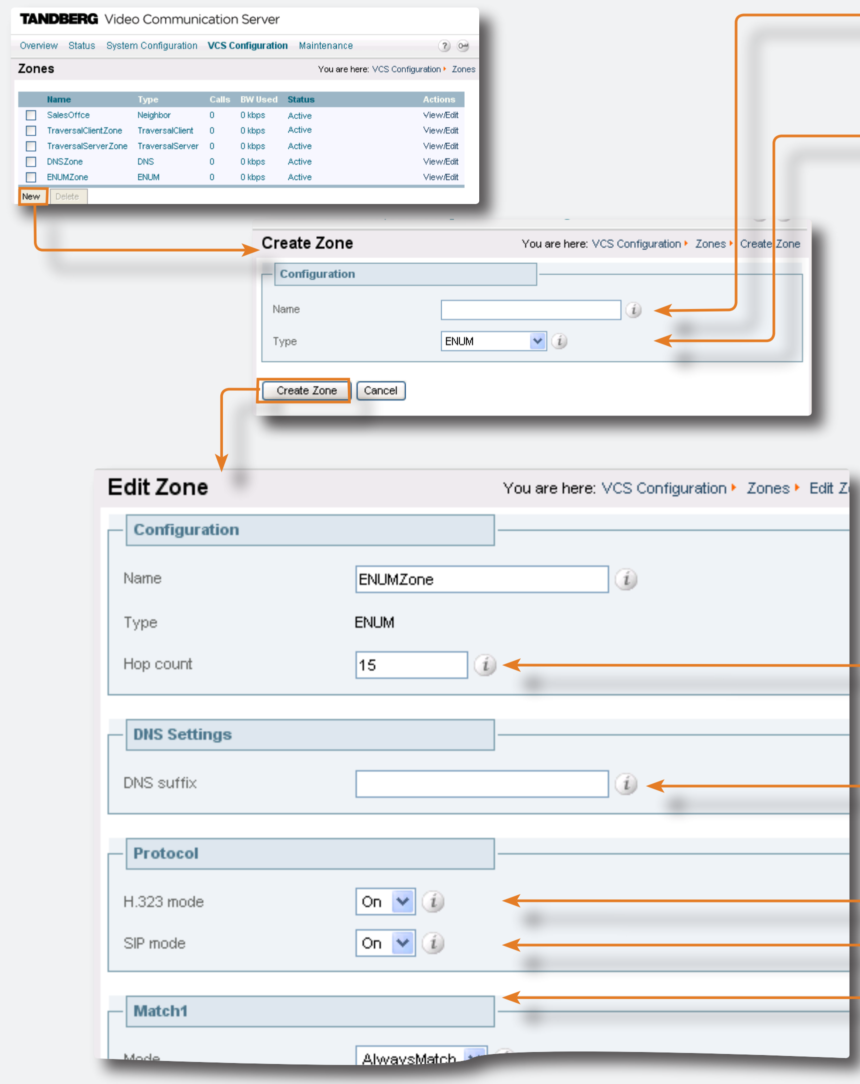
  Enter the zone Name and select a Type of ENUM.

  Click Create Zone.
  You will be taken to the Edit Zone page.
- xCommand ZoneAdd
- xConfiguration Zones Zone [1..200]

Any number of ENUM zones may be configured on the VCS.

You should configure at least one ENUM zone for each DNS suffix that your endpoints may use.

Normal zone pattern matching and prioritization rules will apply to ENUM zones.



Name

Assigns a name to this zone.

Type

For ENUM zones, this will be ENUM.

Hop count

Specifies the hop count to be used when sending an alias search request to this zone. If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.

DNS suffix

The DNS zone that is to be queried for a NAPTR record. This suffix is appended to the transformed E.164 number in an attempt to find a matching NAPTR record.

H.323 mode

Determines whether or not H.323 records will be looked up for this zone.

SIP mode

Determines whether or not SIP records will be looked up for this zone.

Match1 - Match5

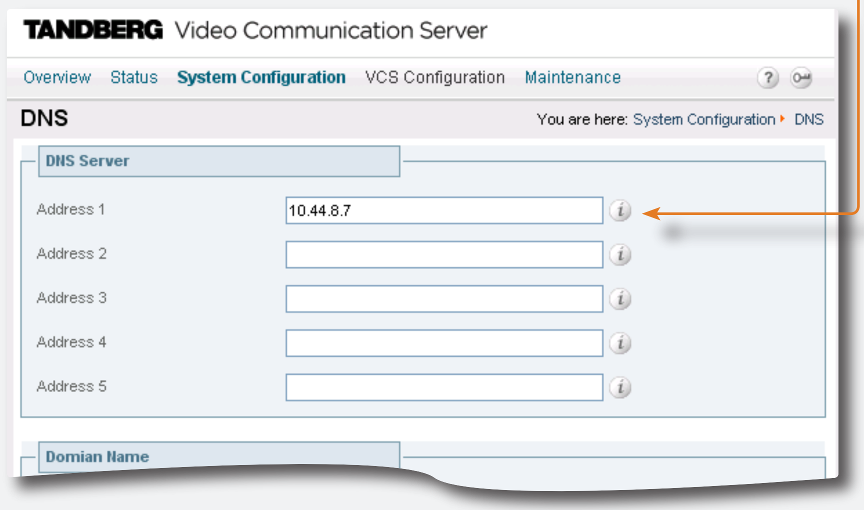
These sections allow you to specify any filtering criteria and/or transforms you wish to apply to this zone. See Configuring Matches for ENUM zones and Configuring Transforms for ENUM zones for full information on how the Match options can be applied.

ENUM Dialing for Outgoing Calls

Configuring DNS Servers

To configure the DNS servers to be used by the VCS when querying DNS:

- *System Configuration > DNS*.
  You will be taken to the DNS page.
- `xConfiguration IP DNS Server`



Address 1 to Address 5

Enter the IP address(es) of up to 5 DNS servers that the VCS will query when attempting to locate a domain.

In order for endpoints registered to the VCS to make outgoing calls using ENUM dialing, you must configure at least one DNS server for the VCS to query. For resilience, you can specify up to five DNS servers.

The DNS server(s) configured here are used as part of both the ENUM dialing and URI dialing processes.

ENUM Dialing

ENUM Dialing for Incoming Calls

Prerequisites

In order for your locally registered endpoints to be reached using ENUM dialing, you must configure a DNS NAPTR record that maps your endpoints' E.164 numbers to their SIP/H.323 URIs. This record must be located at an appropriate DNS domain where it can be found by any systems attempting to reach you via ENUM dialing.

About DNS Domains for ENUM

ENUM relies on the presence of NAPTR records as defined by RFC 2915 [7]. These provide the mapping between E.164 numbers and their SIP/H.323 URIs.

RFC 3761 [8], which is part of a suite of documents that define the ENUM standard, specifies that the domain for ENUM - where the NAPTR records should be located for public ENUM deployments - is e164.arpa. However, use of this domain requires that your E.164 numbers are assigned by an appropriate national regulatory body. Not all countries are yet participating in ENUM, so you may wish to use an alternative domain for your NAPTR records. This domain could reside within your corporate network (for internal use of ENUM) or it could use a public ENUM database such as `http://www.e164.org`.

Configuring DNS NAPTR Records

ENUM relies on the presence of NAPTR records, as defined by RFC 2915 [7]. These are used to obtain an H.323 or SIP URI from an E.164 number.

The record format that the VCS supports is:

- `;; order flag preference service regex replacement`

where:

- `order` and `preference` determine the order in which NAPTR records will be processed. The record with the lowest `order` is processed first, with those with the lowest `preference` being processed first in the case of matching `order`.
- `flag` determines the interpretation of the other fields in this record. Only the value `u` (indicating that this is a terminal rule) is currently supported, and this is mandatory.
- `service` states whether this record is intended to describe E.164 to URI conversion for H.323 or for SIP. Its value must be either `E2U+h323` or `E2U+SIP`.
- `regex` is a regular expression that describes the conversion from the given E.164 number to an H.323 or SIP URI.
- `replacement` is not currently used by the VCS and should be set to `.` (i.e. the full stop character).

Non-terminal rules in ENUM are not currently supported by the VCS. For more information on these, see section 2.4.1 of RFC 3761 [8],

Example

For example, the record:

- `IN NAPTR 10 100 "u" "E2U+h323" "!^(.*)$!h323:\1@example.com!" .`

would be interpreted as follows:

- `10` is the `order`
- `100` is the `preference`
- `u` is the `flag`
- `E2U+h323` states that this record is for an H.323 URI
- `!^(.*)$!h323:\1@example.com!` describes the conversion:
  - `!` is a field separator
  - the first field represents the string to be converted. In this example, `^(.*)$` represents the entire E.164 number
  - the second field represents the H.323 URI that will be generated. In this example, `h323:\1@example.com` states that the E.164 number will be concatenated with `@example.com`. For example, `1234` will be mapped to `1234@example.com`.
- `.` shows that the `replacement` field has not been used.

Calls to and from Unregistered Endpoints

About Unregistered Endpoints

An unregistered endpoint is any device that is not registered with an H.323 gatekeeper or SIP Registrar (e.g. VCS, gatekeeper or Border Controller). Although most calls are made between endpoints each registered with such a system, it is sometimes necessary to place a call to, or receive a call from, an unregistered endpoint.

Calls from an Unregistered Endpoint

An unregistered endpoint can call an endpoint registered with the local VCS.

If there are no firewalls between the unregistered endpoint and the locally registered endpoint, it is possible for the caller to place the call by dialing the locally registered endpoint's IP address. However, we do not recommend that callers are given IP addresses to use as the call may not always be successful (for example if the IP address is private).

Instead, we recommend that callers from unregistered endpoints dial the IP address or the domain name (if configured) of the local VCS, prefixed by the alias they wish to call. The VCS will then resolve the alias and place the call as normal.

Calls to an Unregistered Endpoint

Overview

Calls can be placed from an endpoint registered to the local VCS to an endpoint that is not registered with any system in two ways:

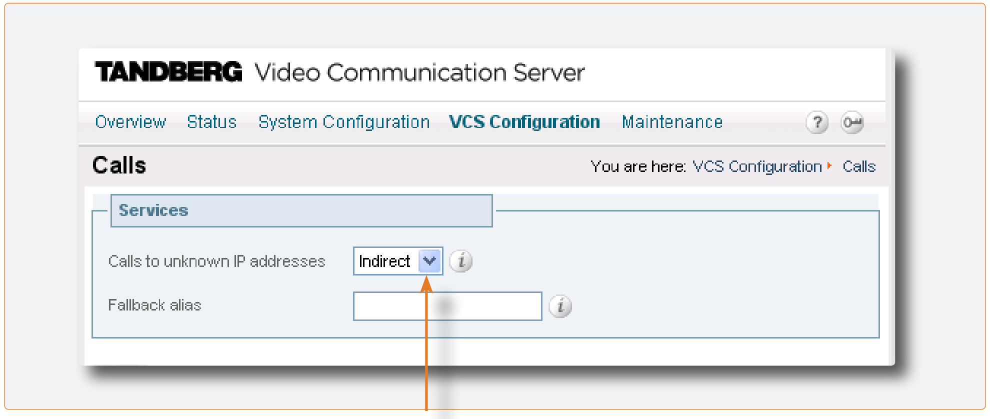
- using an H.323 URI (if the DNS system has been appropriately configured). If URI dialing is used, DNS is queried for a call signaling address and, if found, the call is placed to that address. (See URI Dialing for details of how to configure the Call Signaling SRV Record.)
- dialing its IP address

However, it is sometimes undesirable for a system to be allowed to place a call to an IP address directly. Instead, you may want a neighbor to place the call on behalf of the VCS, or not allow such calls at all. The VCS allows you to configure this behavior.

Configuration

To configure the VCS's behavior when receiving a call for an IP address that is not registered locally:

- *VCS Configuration > Calls*
  You will be taken to the Calls page.
- `xConfiguration Call Services CallsToUnknownIPAddresses`



Calls to Unknown IP Addresses

Determines the way in which the VCS will manage calls to IP addresses which are not registered with it or one of its neighbors.

Direct: A locally registered endpoint will be allowed to make the call to the unknown IP address without the VCS querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system.

Indirect: Upon receiving the call the VCS will check to see if the IP address belongs to one of its locally registered endpoints. If so, it will allow the call. If not, it will query its neighbors for the remote address. If the neighbor's configuration allows it to connect a call to that alias, the VCS will pass the call to that neighbor for completion.

Off: This will not allow any endpoint registered locally to the VCS to call an IP address of any system not also registered locally to that VCS.

Recommended Configuration for Firewall Traversal

When the VCS Border Controller is neighbored with an internal VCS for firewall traversal, you should typically set Calls to unknown IP addresses to Indirect on the internal VCS and Direct on the VCS Border Controller. When a caller inside the firewall attempts to place a call to an IP address outside the firewall, it will be routed as follows:

1. The call will go from the endpoint to the internal VCS with which it is registered.
2. Since the IP address being called is not registered to that VCS, and its Calls to unknown IP addresses setting is Indirect, the VCS will not place the call directly. Instead, it will query its neighbor VCS Border Controller to see if that system is able to place the call on the internal VCS's behalf.
3. The VCS Border Controller receives the call and since its Calls to unknown IP addresses setting is Direct, it will make the call directly to the called IP address.

Fallback Alias

Fallback Alias

Overview

It is possible for the VCS to receive a call that is destined for it but which does not specify an alias. This could be for one of the following reasons:

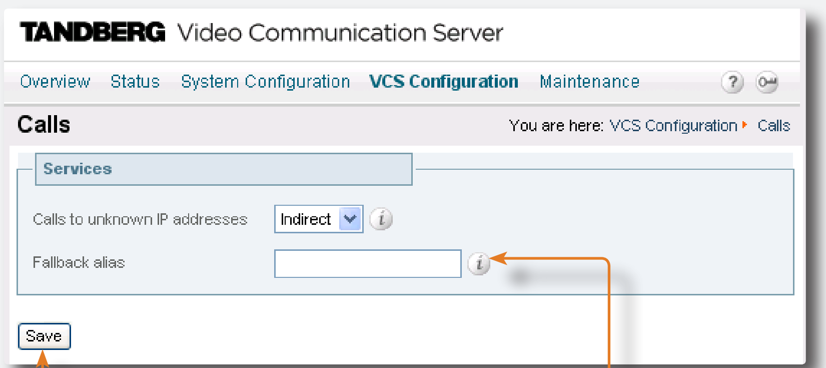
- the caller has dialled the IP address of the VCS directly
- the caller has dialled the domain name without giving an alias as a prefix
- the caller has dialled the IP address or domain name of the VCS prefixed by the VCS's system name as an alias.

Normally such calls would be disconnected. However, the VCS allows you to specify an alias to which all such calls should be routed. This alias is known as the Fallback Alias.

Configuration

To configure the Fallback Alias:

- *VCS Configuration > Calls*.
  You will be taken to the Calls page.
- `xConfiguration Call Services Fallback Alias`



Example Use of a Fallback Alias

You may wish to configure your Fallback Alias to be that of your receptionist, so that all calls that do not specify an alias will still be answered personally and can then be redirected appropriately.

For example, Example Inc. has the domain of example.com. The endpoint at reception has the alias reception@example.com.

They configure their VCS with a fallback alias of reception@example.com. This means that any calls made directly to example.com (i.e. without being prefixed by an alias), are forwarded to reception@example.com, where the receptionist answers the call and directs it appropriately.

Some endpoints do not allow users to enter an alias and an IP address to which the call should be placed.

Save

Click here to save your changes.

Fallback alias

Enter the alias to which you want to forward all calls that do not already specify an alias.

If no fallback alias is configured, calls that do not specify an alias will be disconnected.

Disconnecting calls

Overview

About the Call Control API

The VCS provides a third party call control API. Currently this API supports the following feature:

- disconnecting a call.

Identifying a Particular Call

Each call that passes through the VCS is assigned a call ID number and a call serial number, both of which can be referenced when disconnecting a call via the CLI.

Call ID Number

The VCS assigns each call currently in progress a different call ID number. The ID numbers start at 1 and go up to the maximum number of calls allowed on that system.

Each time a call is made, the VCS will assign that call the lowest available call ID number. For example, if there is already a call in progress with an ID of 1, the next call will be assigned an ID of 2. If call 1 is then disconnected, the third call to be made will be assigned an ID of 1.

The call ID number is not therefore a unique identifier: while no two calls in progress at the same time will have the same call ID number, the same number will be assigned to more than one call over time.

Call Serial Number

The VCS assigns a unique serial number to every call passing through it. No two calls on a VCS will ever have the same serial number. However, a single call passing through a number of VCSs will be identified by a different serial number on each system.

Obtaining the Call ID/Serial Number

To control calls using the CLI, you must reference the call using either its call ID or serial number. These can be obtained using the command:

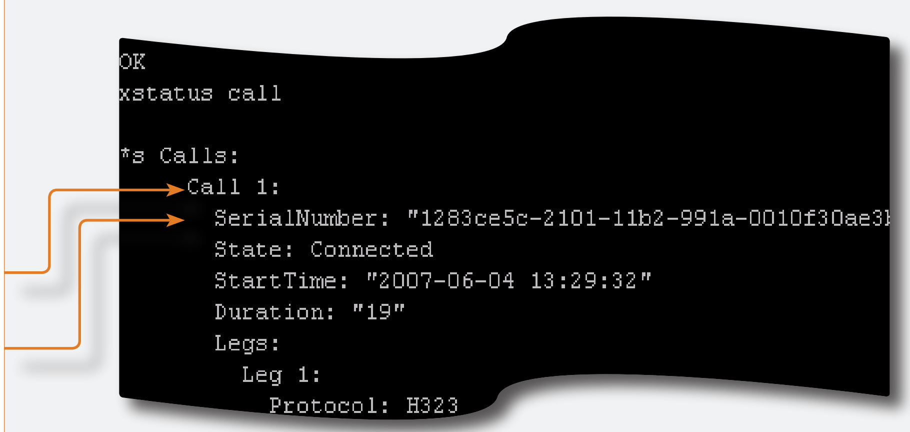
- `xStatus Calls`

This will return details of each call currently in progress in order of their call ID number. The second line of each entry will list the call serial number.

Call ID number

Call serial number

The VCS web UI does not use the call ID number. Calls are identified using their call serial number only.

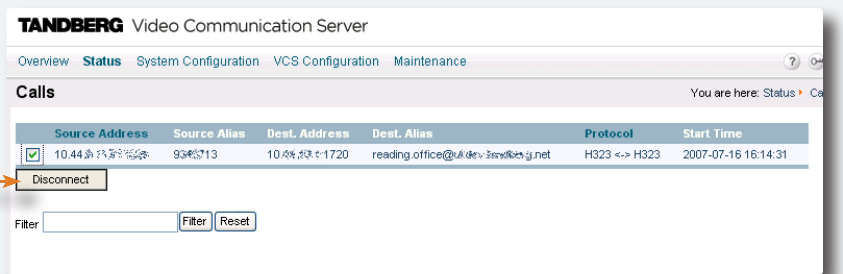


Disconnecting calls

Disconnecting a Call via the Web Interface

To disconnect one or more existing call via the web interface:

- *Status > Calls*.
  You will be taken to the Calls page.



Disconnect

Check the box next to the call(s) you wish to terminate and select Disconnect.

Disconnecting a Call via the CLI

To disconnect an existing call using the CLI, you must first obtain either the call ID number or the call serial number. Then use either one of the following commands as appropriate:

- xCommand DisconnectCall Call: <ID number>
- xCommand DisconnectCall CallSerialNumber: <serial number>

While it is quicker to use the call ID number to reference the call to be disconnected, there is a risk that in the meantime the call has already been disconnected and the call ID assigned to a new call. For this reason, the VCS also allows you to reference the call using the longer but unique call serial number.

Issues when Disconnecting SIP Calls

The call disconnection API works differently for H.323 and SIP calls due to differences in the way the protocols work.

For H.323 calls, the Disconnect command will actually disconnect the call.

For SIP calls, the Disconnect command will cause the VCS to release all resources used for the call and the call will appear on the system as disconnected. However, SIP calls are peer-to-peer and as a SIP proxy the VCS has no authority over the endpoints. Although releasing the resources may have the side-effect of disconnecting the SIP call, it is also possible that the call signaling, media or both may stay up (depending on the type of call being made). The call will not actually disconnect until the SIP endpoints involved have also cleared their resources.

Endpoints that support RFC 4028 [14] have a call refresh timer which should cause them to clear the resources of any hung SIP calls after a certain period of time. This includes all TANDBERG endpoints.

Firewall Traversal Overview

About Firewall Traversal

The purpose of a firewall is to control the IP traffic entering your network. Firewalls will generally block unsolicited incoming requests, meaning that any calls originating from outside your network will be prevented. However, firewalls can be configured to allow outgoing requests to certain trusted destinations, and to allow responses from those destinations. This principle is used by TANDBERG's Expressway™ solution to enable secure traversal of any firewall.

The Expressway™ solution consists of:

- a VCS Border Controller or Border Controller located outside the firewall on the public network or DMZ, which acts as the firewall traversal server,
- a VCS, Gatekeeper, MXP endpoint or other traversal-enabled endpoint located on the private network, which acts as the firewall traversal client.

The two systems work together to create an environment where all connections between the two are outbound, i.e. established from the client to the server, and thus able to successfully traverse the firewall.

How does it work?

The traversal client constantly sends a probe via the firewall to a designated port on the traversal server. This keeps a connection alive between the client and server. When the traversal server receives an incoming call for the traversal client, it uses this existing connection to send an incoming call request to the client. The client then initiates a connection to the server and upon receipt the server responds with the incoming call. This process ensures that from the firewall's point of view, all connections are initiated from the traversal client inside the firewall out to the traversal server.

VCS and Firewall Traversal

VCS as a Firewall Traversal Client

Your VCS can act as a firewall traversal client on behalf of SIP and H.323 endpoints registered to it, and any gatekeepers that are neighbored with it.

In order to act as a firewall traversal client, the VCS must be configured with information about the system(s) that will be acting as its firewall traversal server. See the section on Configuring the VCS as a Traversal Client for full details on how to do this.

The firewall traversal server used by the VCS can be another VCS with the Border Controller option enabled, or a TANDBERG Border Controller.

VCS as a Firewall Traversal Server

In addition to being a firewall traversal client, the VCS can be enabled to act as a firewall traversal server. With this option enabled, the VCS will act as a traversal server for other TANDBERG systems and any traversal-enabled endpoints that are registered directly to it. It can also provide STUN Discovery and STUN relay services to endpoints with STUN clients.

- To enable server-side firewall traversal for other systems, you must create and configure a new traversal server zone on the VCS for every system that is its traversal client. See Configuring the VCS as a traversal server for details on how to do this.
- To enable server-side firewall traversal for traversal-enabled endpoints (i.e. TANDBERG MXP endpoints and any other endpoints that support the ITU H.460.18 and H.460.19 standards) no additional configuration is required. See Configuring traversal for endpoints for more information on the options available.
- To enable STUN Discovery and STUN Relay services, see STUN Services.
- To reconfigure the default ports used by the VCS Border Controller, see Configuring traversal server Ports.

To use the VCS as a traversal server, you must install the Border Controller option key on your system. Contact your TANDBERG representative for further information.

In order for firewall traversal to function correctly, the VCS Border Controller must have a traversal server zone configured on it for each client that is connecting to it. Likewise, each VCS client must have a traversal client zone configured on it for each server that it is connecting to. The ports and protocols configured for each pair of zones must be the same. Because the VCS Border Controller listens for connections from the client on a specific port, we recommend that you create the traversal server zone before you create the traversal client zone.

Firewall Traversal Protocols and Ports

Overview

Ports play a vital part in firewall traversal configuration. The correct ports must be set on the VCS Border Controller, traversal client and firewall in order for connections to be permitted.

Ports are initially configured on the VCS Border Controller and then advised to the firewall administrator and the traversal client administrator, who must then configure their systems to connect to these specific ports on the server. The only port configuration that is done on the client is the range of ports it uses for outgoing connections; the firewall administrator will need to know this information so that if necessary they can configure the firewall to allow outgoing connections from those ports.

Process

- Each traversal client connects via the firewall to a unique port on the VCS Border Controller.
- The server identifies each client by the port on which it receives the connection, and the Authentication credentials provided by the client.
- Once established, the client constantly sends a probe to the VCS Border Controller via this connection in order to keep the connection alive.
- When the VCS Border Controller receives an incoming call for the client, it uses this initial connection to send an incoming call request to the client.
- The client then initiates a connection to the server. The ports used for the call will differ for signaling and media, and will depend on the protocol being used (i.e. SIP, Assent or H.460.18/19).

Ports for Initial Connections from Traversal Clients

Each traversal server zone specifies an H.323 port and a SIP port to be used for the initial connection from the client.

Each time you configure a new traversal server zone on the VCS, you will be allocated default port numbers for these connections:

- H.323 ports will start at 6001 and increment by 1 for every new traversal server zone
- SIP ports will start at 7001 and increment by 1 for every new traversal server zone.

You can change these default ports if necessary but you must ensure that the ports are unique for each traversal server zone.

Once the H.323 and SIP ports have been set on the VCS Border Controller, matching ports must be configured on the corresponding traversal client.

The default port used for the initial connections from MXP endpoints is the same as that used for standard RAS messages, i.e. UDP/1719. While it is possible to change this port on the VCS server, most endpoints will not support connections to ports other than UDP/1719. We therefore recommend that this be left as the default.

H.323 Firewall Traversal Protocols

The VCS supports two different firewall traversal protocols for H.323: Assent and H.460.18/H.460.19.

- Assent is TANDBERG's proprietary protocol.
- H.460.18 and H.460.19 are ITU standards which define protocols for the firewall traversal of signaling and media respectively. These standards are based on the original TANDBERG Assent protocol.

In order for a traversal server and traversal client to communicate, they must be using the same protocol.

The two protocols each use a slightly different range of ports.

Assent Ports

For connections to the VCS Border Controller using the Assent protocol, the default ports are:

Call signaling

- UDP/1719: listening port for RAS messages
- TCP/2776: listening port for H.225 and H.245 protocols

Media

- UDP/2776: RTP media port
- UDP/2777: RTCP media control port

H.460.18/19 Ports

For connections to the VCS Border Controller using the H.460.18/19 protocols, the default ports are:

Call signaling

- UDP/1719: listening port for RAS messages
- TCP/1720: listening port for H.225 protocol
- TCP/2777: listening port for H.245 protocol

Media

- UDP/2776: RTP media port
- UDP/2777: RTCP media control port

SIP Ports

Call signaling

SIP call signaling uses the same port as used by the initial connection between the client and server.

Media

Where the traversal client is a VCS or Gatekeeper, SIP media uses Assent to traverse the firewall . The default ports are the same as for H.323, i.e.:

- UDP/2776: RTP media port
- UDP/2777: RTCP media control port

Firewall Traversal

Firewall Traversal Protocols and Ports

Ports for Connections out to the Public Internet

In situations where the VCS Border Controller is attempting to connect to an endpoint on the public internet, you will not know the exact port(s) on the endpoint to which the connection will be made. This is because the ports to be used are determined by the endpoint and advised to the VCS Border Controller only once the server has located the endpoint on the public internet. This may cause problems if your VCS Border Controller is located within a DMZ (i.e. there is a firewall between the VCS Border Controller and the public internet) as you will not be able to specify in advance rules that will allow you to connect out to the endpoint's ports.

You can however specify the ports on the VCS Border Controller that will be used for calls to endpoints on the public internet so that your firewall administrator can allow connections via these ports. The ports that can be configured for this purpose are:

H.323

- UDP/1719: signaling
- UDP/50,000-51200: media
- TCP/15,000-19999: signaling

SIP

- UDP/5060 (default): signaling
- UDP/50,000-51200: media
- TCP: a temporary port is allocated

STUN Ports

The VCS Border Controller can be enabled to provide STUN services (STUN Relay and STUN Binding Discovery) that can be used by SIP endpoints which support the ICE firewall traversal protocol.

The ports used by these services are configurable via:

- *VCS Configuration > Border Controller > STUN*
- `xConfiguration Traversal Server STUN`

The ICE clients on each of the SIP endpoints must be able to discover these ports, either via SRV records in DNS or by direct configuration.

Firewall Configuration

In order for Expressway™ firewall traversal to function correctly, the firewall must be configured to:

- allow initial outbound traffic from the client to the ports being used by the VCS Border Controller
- allow return traffic from those ports on the VCS Border Controller back to the originating client.

TANDBERG offers a downloadable tool, the Expressway Port Tester, that allows you to test your firewall configuration for compatibility issues with your network and endpoints. It will advise if necessary which ports may need to be opened on your firewall in order for the Expressway™ solution to function correctly. Contact your TANDBERG representative for more information.

We recommend that you turn off any H.323 and SIP protocol support on the firewall: these are not needed in conjunction with the TANDBERG Expressway™ solution and may interfere with its operation.

Firewall Traversal and Authentication

Overview

In order to control usage of the VCS as a traversal server, each VCS or Gatekeeper that wishes to be its client must first authenticate with it.

Upon receiving the initial connection request from the traversal client, the VCS Border Controller asks the client to authenticate itself by providing a username and password. The server then looks up the username and password in its own authentication database. If a match is found, the VCS server will accept the request from the client.

The settings used for authentication depend on the combination of client and server being used. These are detailed in the table opposite.

When acting as a VCS Border Controller, authentication is required from all VCS and Gatekeeper clients regardless of the VCS's Authentication Mode setting. This setting will however still determine whether or not endpoint clients are required to authenticate.

Client Type and Client Settings	Server Type and Server Settings
VCS • The VCS client provides its Authentication Username and Authentication Password. These are set on the client via *VCS Configuration > Authentication > Configuration*.	VCS Border Controller • The traversal server zone for that client must be configured with the client's Authentication Username. This is set via *VCS Configuration > Zones > Edit Zone*. • There must also an entry in the server's authentication database with the corresponding username and password.
Endpoint Client • The endpoint client provides its Authentication ID and Authentication Password.	VCS Border Controller • There must be an entry in the server's authentication database with the corresponding username and password.
Gatekeeper Client • The Gatekeeper client looks up its System Name in its own authentication database and retrieves the password for that name. It then provides this name and password.	VCS Border Controller • The traversal server zone for the Gatekeeper client must be configured with the Gatekeeper's System Name in the Authentication Username field. This is set via *VCS Configuration > Zones > Edit Zone*. • There must be an entry in the server's authentication database with the corresponding username and password.
VCS • If Authentication is On on the Border Controller, the VCS client provides its Authentication Username and Authentication Password. These are set on the client via *VCS Configuration > Authentication > Configuration*. • If the Border Controller is in Assent mode, the VCS client provides its Authentication Username. This is set on the client via *VCS Configuration > Authentication > Configuration*.	Border Controller • If Authentication is On on the Border Controller, there must be an entry in the Border Controller's authentication database that matches the VCS client's Authentication Username and Authentication Password. • If the Border Controller is in Assent mode, the traversal zone configured on the Border Controller to represent the VCS client must use the client's Authentication Username in the Assent Account name field. This is set on the Border Controller via *TraversalZone > Assent > Account name*.

Configuring the VCS as a Traversal Client

Overview

To enable your VCS to act as a traversal client on behalf of its endpoints and neighbor gatekeepers, you must create a connection between it and a traversal server (e.g. a VCS Border Controller).

You do this by adding a new traversal client zone and configuring it with the details of the traversal server.

Adding a New Traversal Client Zone

- *VCS Configuration > Zones*.
  You will be taken to the Zones page.
  Select New.
  You will be taken to the Create Zone page.
- xCommand ZoneAdd

Name

Enter the name you wish to give to this zone. The name acts as a unique identifier, allowing you to distinguish between zones of the same type.

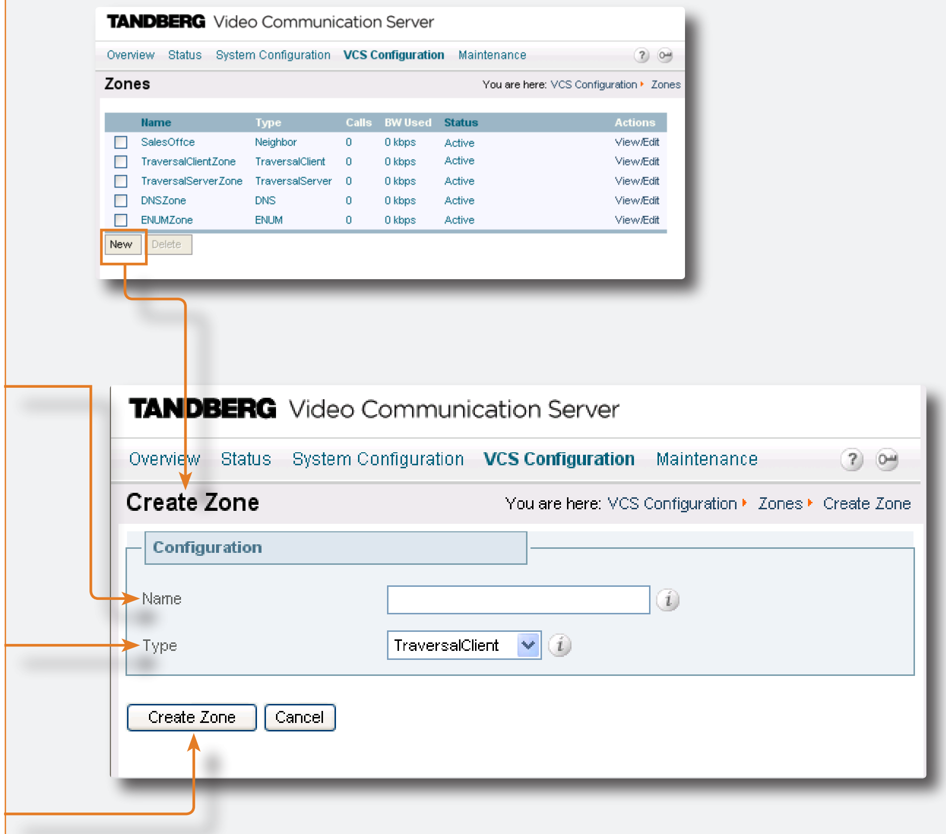
Type

From the Type drop-down menu, select TraversalClient.

Create Zone

Click here to create the zone. You will be taken directly to the Edit Zone page, where you can configure the traversal client zone as required.

You can create more than one traversal client zone if you wish to connect to multiple traversal servers.



Configuring the VCS as a Traversal Client

Configuring a Traversal Client Zone

- *VCS Configuration > Zones*.
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zone page.
- `xConfiguration Zones Zone`

Retry interval

Specifies the interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried.

H.323 mode

Determines whether H.323 calls will be allowed to and from this zone.

H.323 protocol

Determines which of the two firewall traversal protocols to use for calls to the traversal server.

H.323 port

Specifies the port on the traversal server to be used for H.323 firewall traversal calls.

SIP mode

Determines whether SIP calls will be allowed to and from this zone.

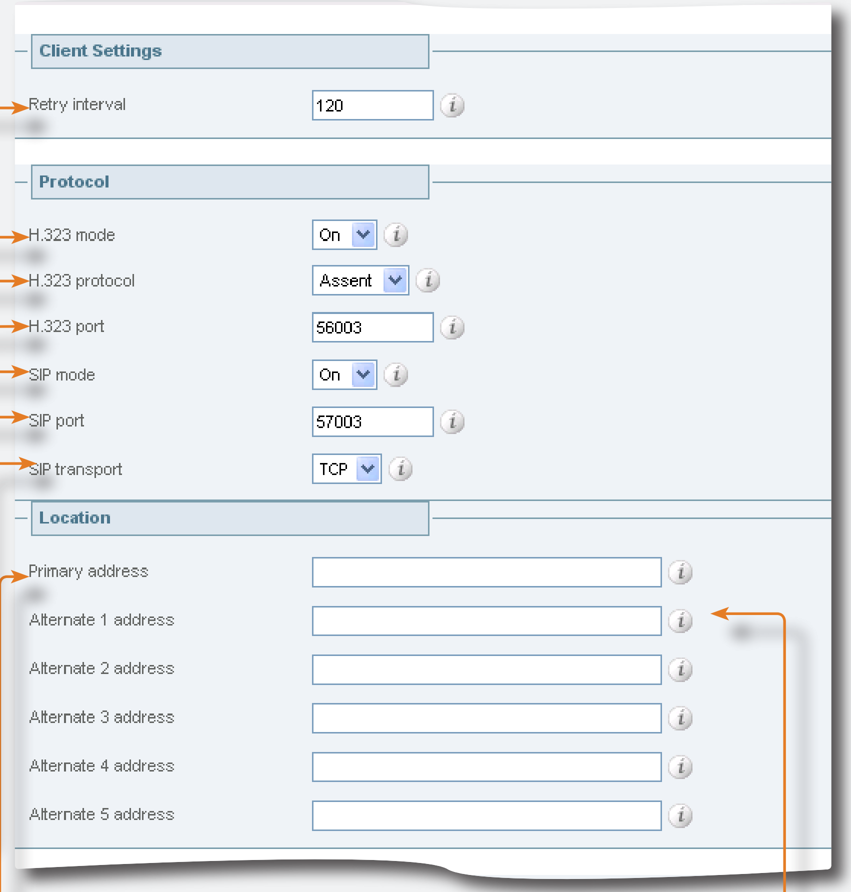
SIP port

Specifies the port on the traversal server to be used for SIP calls from this VCS

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal server.

Remember to Save your changes.



Primary address

Specifies the IP address or FQDN of the traversal server.

Alternate 1 - Alternate 5 Address

Specifies the IP addresses or FQDNs of any alternates configured on the traversal server.

Configuring the VCS as a Traversal Server

Overview

The VCS has an optional Border Controller feature. Once this has been enabled, you will be able to:

- Allow your VCS to act as a traversal server for other VCSs and TANDBERG Gatekeepers. You do this by adding a new traversal server zone on the VCS, and configuring it with details of the traversal client.
- Provide firewall traversal for any TANDBERG MXP endpoints registered directly with it. You can configure the protocols and ports that will be used.
- Enable and configure STUN services.
- Configure the ports used specifically for firewall traversal services.

The following sections describe how to configure each of the above options.

Adding a New Traversal Server Zone

- *VCS Configuration > Zones*.
  You will be taken to the Zones page.
  Select New.
  You will be taken to the Create Zone page.
- `xCommand ZoneAdd`

Name

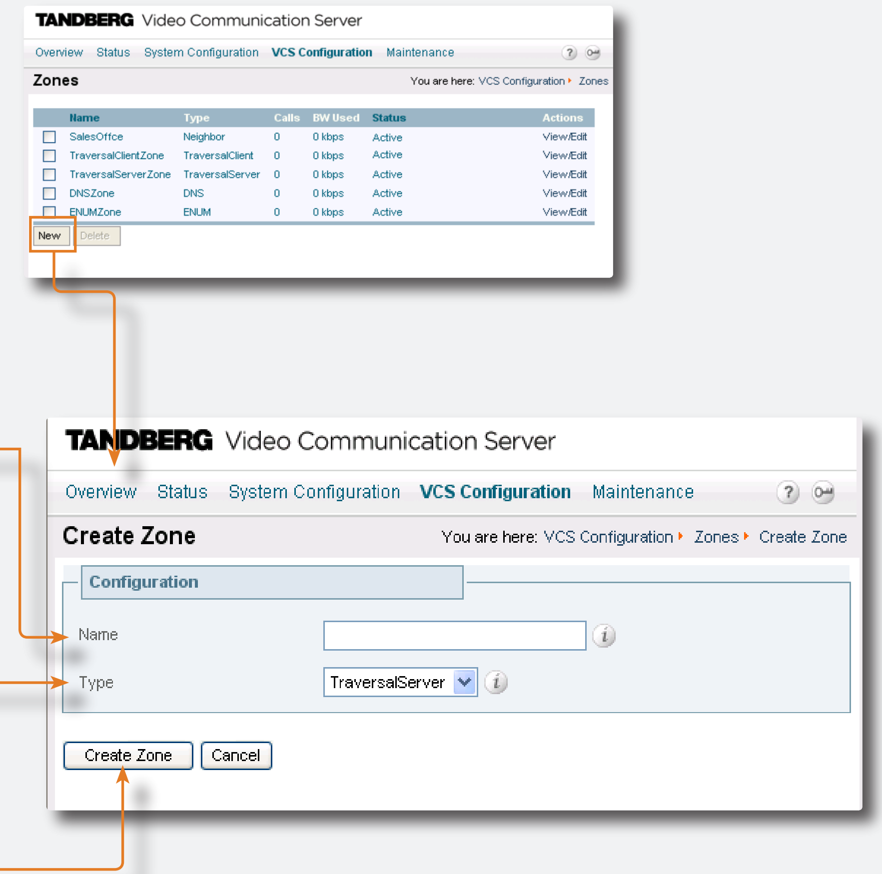
Enter the name you wish to give to this zone. The name acts as a unique identifier, allowing you to distinguish between zones.

Type

From the Type drop-down menu, select TraversalServer.

Create Zone

Click here to create the zone. You will be taken directly to the Edit Zone page, where you can configure the traversal server zone as required.



Firewall Traversal

Configuring the VCS as a Traversal Server

Configuring a Traversal Server Zone

- *VCS Configuration > Zones*.
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zones page.
- `xConfiguration Zones Zone`

Authentication username

If the traversal client is a VCS, this must be the VCS's Authentication Username. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name.

H.323 mode

Determines whether H.323 calls will be allowed to and from the traversal client.

H.323 protocol

Determines which of the two firewall traversal protocols will be used for calls through the firewall, to and from the client. The same protocol must be used by the client.

H.323 port

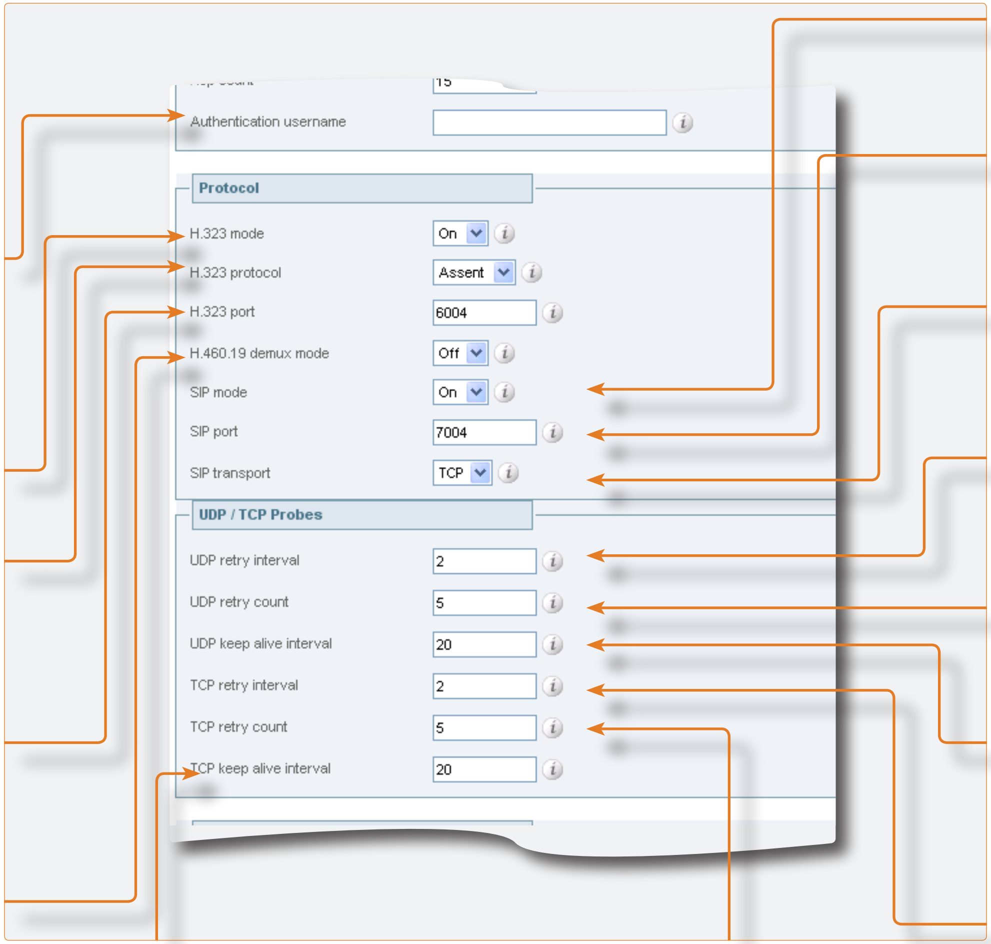
Specifies the port on the VCS Border Controller to be used for H.323 connections from the client.

H.460.19 demux mode

Determines whether or not the same two ports can be used for media by two or more calls from the traversal client.

On: allows use of the same two ports for media for all calls.

Off: each call will use a separate pair of ports for media.



TCP keep alive interval

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

TCP retry count

Sets the number of times the traversal client will attempt to send a TCP probe to the VCS.

SIP mode

Determines whether SIP calls will be allowed to and from the traversal client.

SIP port

Specifies the port on the VCS Border Controller to be used for SIP calls from this traversal client.

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal client.

UDP retry interval

Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the VCS Border Controller.

UDP retry count

Sets the number of times the traversal client will attempt to send a UDP probe to the VCS Border Controller.

UDP keep alive interval

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

TCP retry interval

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the VCS.

Configuring the VCS as a Traversal Server

Configuring Traversal for Endpoints

Traversal-enabled H.323 endpoints can register directly with the VCS Border Controller and use it for firewall traversal.

To configure the options for these endpoints:

- *VCS Configuration > Border Controller > Locally Registered Endpoints*
  You will be taken to the Locally Registered Endpoints page.
- `xConfiguration Zones LocalZone Traversal H323`

H.323 Assent mode

Determines whether or not H.323 calls using Assent mode for firewall traversal will be allowed.

H.460.18 mode

Determines whether or not H.323 calls using H.460.18/19 mode for firewall traversal will be allowed.

H.460.19 demux mode

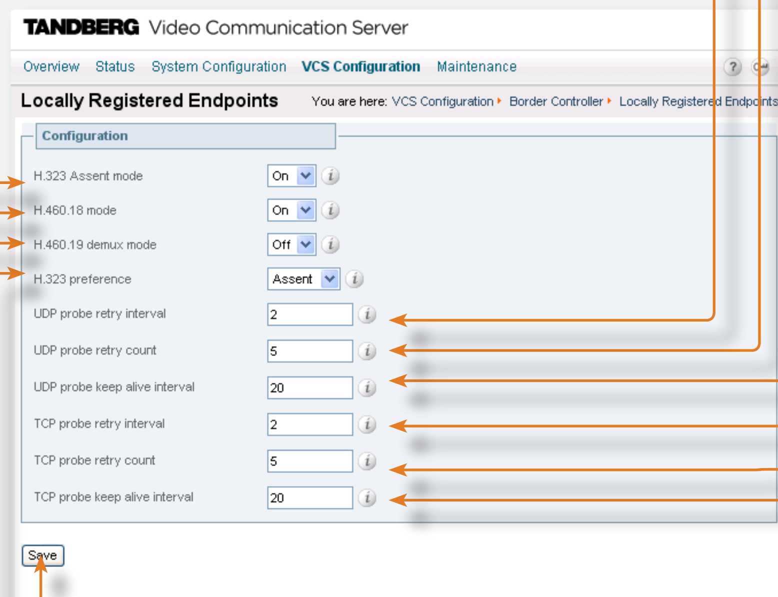
Determines whether the VCS will operate in Demultiplexing mode for calls from locally registered endpoints.

On: allows use of the same two ports for all calls.

Off: Each call will use a separate pair of ports for media.

H.323 preference

If an endpoint supports both Assent and H.460.18 protocols, this setting determines which the VCS uses.



UDP probe retry interval

Sets the frequency (in seconds) with which locally registered endpoints will send a UDP probe to the VCS Border Controller.

UDP probe retry count

Sets the number of times locally registered endpoints will attempt to send a UDP probe.

UDP probe keep alive interval

Sets the interval (in seconds) with which locally registered endpoints will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

TCP probe retry interval

Sets the frequency (in seconds) with which locally registered endpoints will send a TCP probe to the VCS.

TCP probe retry count

Sets the number of times locally registered endpoints will attempt to send a TCP probe to the VCS.

TCP probe keep alive interval

Sets the interval (in seconds) with which locally registered endpoints will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

Save

Click here to save your settings.

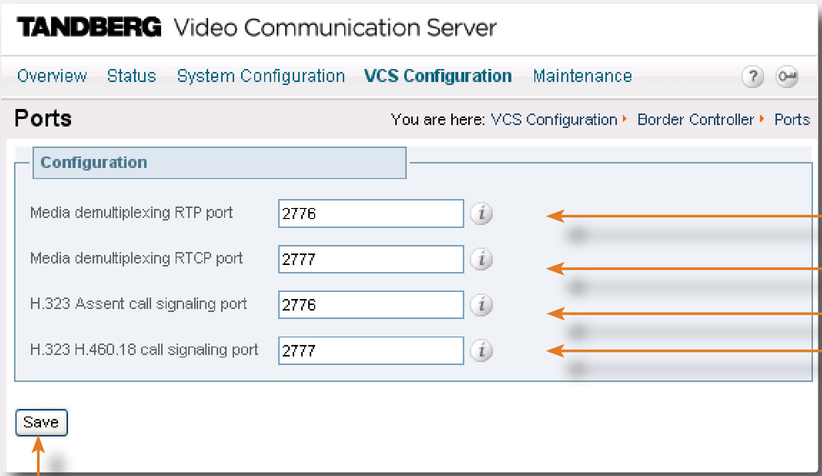
Configuring the VCS as a Traversal Server

Configuring Traversal Server Ports

The VCS has specific listening ports assigned for connections with the firewall. In most cases the default ports should be used. However, you have the option to change these ports if necessary.

To configure the VCS traversal server ports:

- *VCS Configuration > Border Controller > Ports*
  You will be taken to the Ports page.
- xConfiguration Traversal Server Media
- xConfiguration Traversal Server H.323



Media demultiplexing RTP port

Specifies the port on the VCS to be used for demultiplexing RTP media.

Media demultiplexing RTCP port

Specifies the port on the VCS to be used for demultiplexing RTCP media.

H.323 Assent call signaling port

Specifies the port on the VCS to be used for Assent signaling.

H.323 H.460.18 call signaling port

Specifies the port on the VCS to be used for H.460.18 signaling.

Save

Click here to save your settings.

STUN Services

About STUN

STUN is a network protocol that enables a SIP or H.323 client to communicate via UDP or TCP from behind a NAT firewall.

The VCS Border Controller can be configured to provide two types of STUN services to traversal clients. These services are STUN Binding Discovery and STUN Relay.

For detailed information on the base STUN protocol and the Binding Discovery service, refer to “Session Traversal Utilities for (NAT) (STUN)” [11].

For detailed information on the STUN Relay service, refer to “Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN)” [12].

About ICE

Currently, the most likely users of STUN services are ICE endpoints.

ICE (Interactive Connectivity Establishment) is a collaborative algorithm that works together with STUN services (and other NAT traversal techniques) to allow clients to achieve firewall traversal. The individual techniques on their own may allow traversal in certain network topologies but not others. Also some techniques maybe less efficient than others, involving extra hops (e.g. STUN Relay).

ICE involves the collecting of potential (candidate) points of contact (IP address and port combination) via each of the traversal techniques, the verification of peer-to-peer connectivity via each of these points of contact and then the selection of the “best” successful candidate point of contact to use.

STUN Binding Discovery

The STUN Binding Discovery service provides information back to the client about the binding allocated by the NAT firewall being traversed.

How it works

A client behind a NAT firewall sends a STUN discovery request via the firewall to the VCS Border Controller, which has been configured as a STUN discovery server. Upon receipt of the message, the VCS Border Controller responds to the client with information about the allocated NAT binding, i.e. the public IP address and the ports being used.

The client can then provide this information to other systems which may want to reach it, allowing it to be found even though it is not directly available on the public internet.

The endpoint will only be reachable if the firewall has the Endpoint-Independent Mapping behavior as described in RFC 4787 [13].

STUN Relay

The STUN Relay service (formerly known as TURN) allows a client to ask for data to be relayed to it from specific remote peers via the relay server and through a single connection between the client and the relay server.

How it works

A client behind a NAT firewall sends a STUN Allocate request to the VCS Border Controller which is acting as the STUN relay server. The sending of this request opens a binding on the firewall. Upon receipt of the request, the VCS Border Controller opens a public IP port on behalf of the client, and reports back to the client this IP address and port, as well as details of the firewall binding. The client can then provide this IP address and port to other systems which may want to reach it.

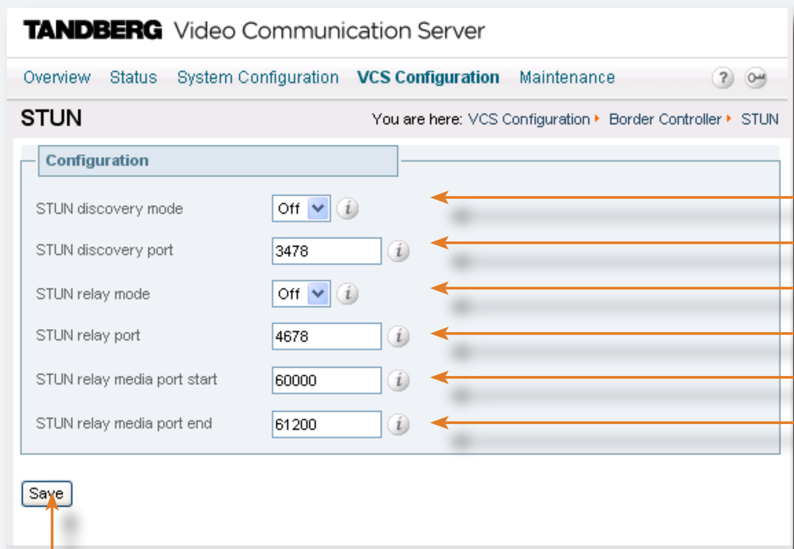
The client can restrict the remote address and ports from which the relay should forward on media. Any incoming calls to this IP address and port on the VCS server are relayed via the allocated binding on the NAT to the client.

STUN Services

Configuring STUN Services

To configure the STUN Binding Discovery and STUN Relay services:

- *VCS Configuration > Border Controller > STUN.*
  You will be taken to the STUN page.
- `xConfiguration Traversal Server STUN`



STUN discovery mode
Determines whether the VCS will offer STUN Discovery services to traversal clients.

STUN discovery port
Specifies the port on the VCS on which it will be listening for STUN Discovery requests.

STUN relay mode
Determines whether the VCS will offer STUN Relay services to traversal clients.

STUN relay port
Specifies the port on the VCS on which it will be listening for STUN relay requests.

STUN relay media port start
Specifies the lower port in the range to be used for STUN media relay.

STUN relay media port end
Specifies the upper port in the range to be used for STUN media relay.

Save
Click here to save your changes.

Overview

About Bandwidth Control

The TANDBERG VCS allows you to control the use of bandwidth by endpoints on your network. This is done by grouping endpoints into subzones, and then applying limits to the bandwidth that can be used:

- within each subzone
- between a subzone and another subzone
- between a subzone and a zone.

Bandwidth limits may be set on a call-by-call basis and/or on a total concurrent usage basis. This flexibility allows you to set appropriate bandwidth controls on individual components of your network.

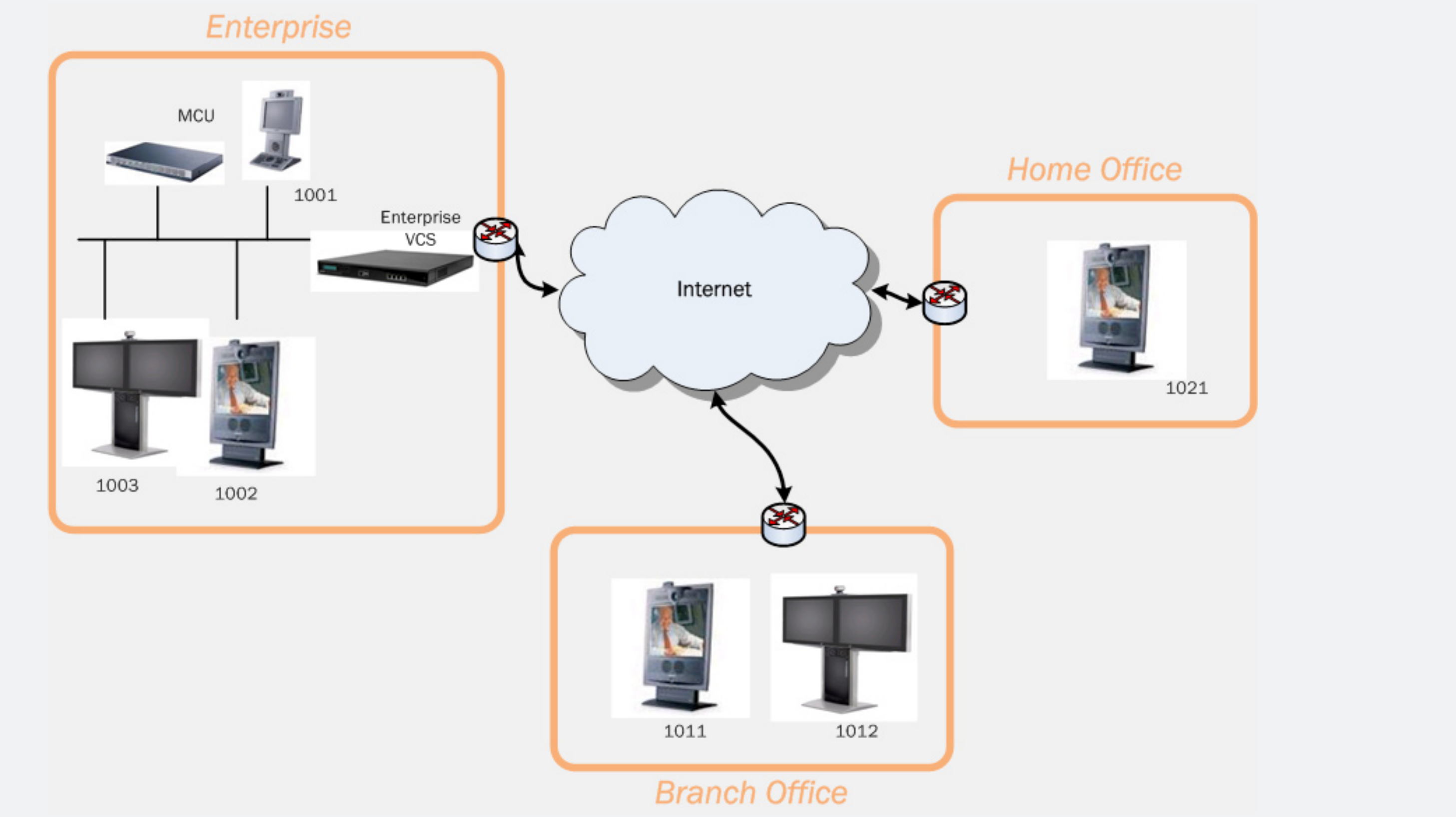
This section describes the different types of subzones and how to add and configure them, and explains how to use Links and Pipes to apply bandwidth controls between subzones and zones.

Example Network Deployment

The diagram below shows a typical network deployment:

- a broadband LAN, where high bandwidth calls are acceptable
- a pipe to the internet with restricted bandwidth
- two satellite offices, Branch and Home, each with their own restricted pipes.

In this example you should create a new subzone for each pool of endpoints, so that you can apply suitable limitations to the bandwidth used within and between each subzone.



Subzones

About Subzones

All endpoints registered with the VCS are part of its Local Zone.

The Local Zone is made up of two or more subzones. The first two subzones are automatically created for you. These are the Default Subzone and the Traversal Subzone. You can create and configure further subzones manually on the basis of endpoints' IP addresses: when an endpoint registers with the VCS its IP address is checked and it is assigned to the appropriate subzone.

The main purpose of subzones is to enable you to control the bandwidth used by various parts of your network.

About the Default Subzone

When an endpoint registers with the VCS, its IP address is checked and it is assigned to the appropriate subzone. If no subzones have been created, or the endpoint's IP address does not match any of the specified subzones, it will be assigned to the Default Subzone.

The use of a Default Subzone on its own (i.e. without any other manually configured subzones) is suitable only if you have uniform bandwidth available between all your endpoints. However, it is possible for a Local Zone to contain two or more different networks with different bandwidth limitations. In this situation, you should configure separate subzones for each different part of the network.

Specifying the IP Address Range of a Subzone

A subzone is defined by specifying a range of IP addresses. The VCS allocates endpoints to a subzone based on their IP address. You specify which IP addresses are associated with the subzone by configuring up to 5 subnets for that subzone.

If an endpoint's IP address matches more than one subnet, it will be allocated to the subnet with the narrowest range.

About the Traversal Subzone

The Traversal Subzone is a conceptual subzone. No endpoints can be registered to the Traversal Subzone; its sole purpose is to allow for the control of bandwidth used by traversal calls.

All traversal calls are deemed to pass through the Traversal Subzone, so by applying bandwidth limitations to the Traversal Subzone you can control how much processing of media the VCS will perform at any one time. These limitations can be applied on a total concurrent usage basis, and/or on a per-call basis.

Default Settings

The VCS is shipped with the Default Subzone, Traversal Subzone and Default Zone already created, and with links between the three. You may delete or amend these default links if you need to model restrictions of your network.

If any of these links have been deleted, they may be automatically restored via:

- `xCommand DefaultLinksAdd`

To restore this link via the web interface, you must recreate it manually. See Creating Links for instructions on how to do this.

Traversal Calls

A traversal call is any call passing through the VCS that includes both the signaling (information about the call) and media (voice and video). The only other type of call is a non-traversal call, where the signaling passes through the VCS but the media goes directly between the endpoints.

Traversal calls include:

- calls that are traversing a firewall
- SIP to H.323 interworking calls
- IPv4 to IPv6 interworking calls.

Traversal calls use more resource that non-traversal calls, and the numbers of each type of call are licensed separately. The VCS has one license for the maximum number of concurrent traversal calls it can take, and another for the maximum number of concurrent non-traversal calls.

A call is "traversal" or "non-traversal" from the point of view of the VCS through which it is being routed at the time. A call between two endpoints may pass through a series of VCSs. Some of these systems may just take the signaling, in which case the call will be a non-traversal call for that VCS. Other systems in the route may need to take the media as well, and so the call will count as a traversal call on that particular VCS.

Bandwidth Consumption of Traversal Calls

Traversal calls between two endpoints within a single subzone on the VCS must, like any other traversal call, pass through the VCS's Traversal Subzone. This means that such calls will consume an amount of bandwidth from the originating subzone's total concurrent allocation that is equal to twice the bandwidth of the call – once for the call from the subzone to the Traversal Subzone, and again for the call from the Traversal Subzone back to the originating subzone.

Calls passing through the Traversal Subzone will consume an amount of bandwidth within the subzone equal to that of the call.

Creating a Subzone

To add a new subzone:

- *VCS Configuration > Local Zone > Subzones*.
  You will be taken to the Subzones page.
  Select New.
  You will be taken to the Create Subzone page.
- `xCommand SubZoneAdd`

Name

Enter the name you wish to assign to the subzone. You will refer to this name when creating Links.

Subnet

Enter the IP address of the subnet. In conjunction with the Prefix, this will define the range of IP addresses that will belong to this subzone.

Prefix

Enter the number of bits of the Subnet IP Address which must match for an IP address to belong in this subzone.

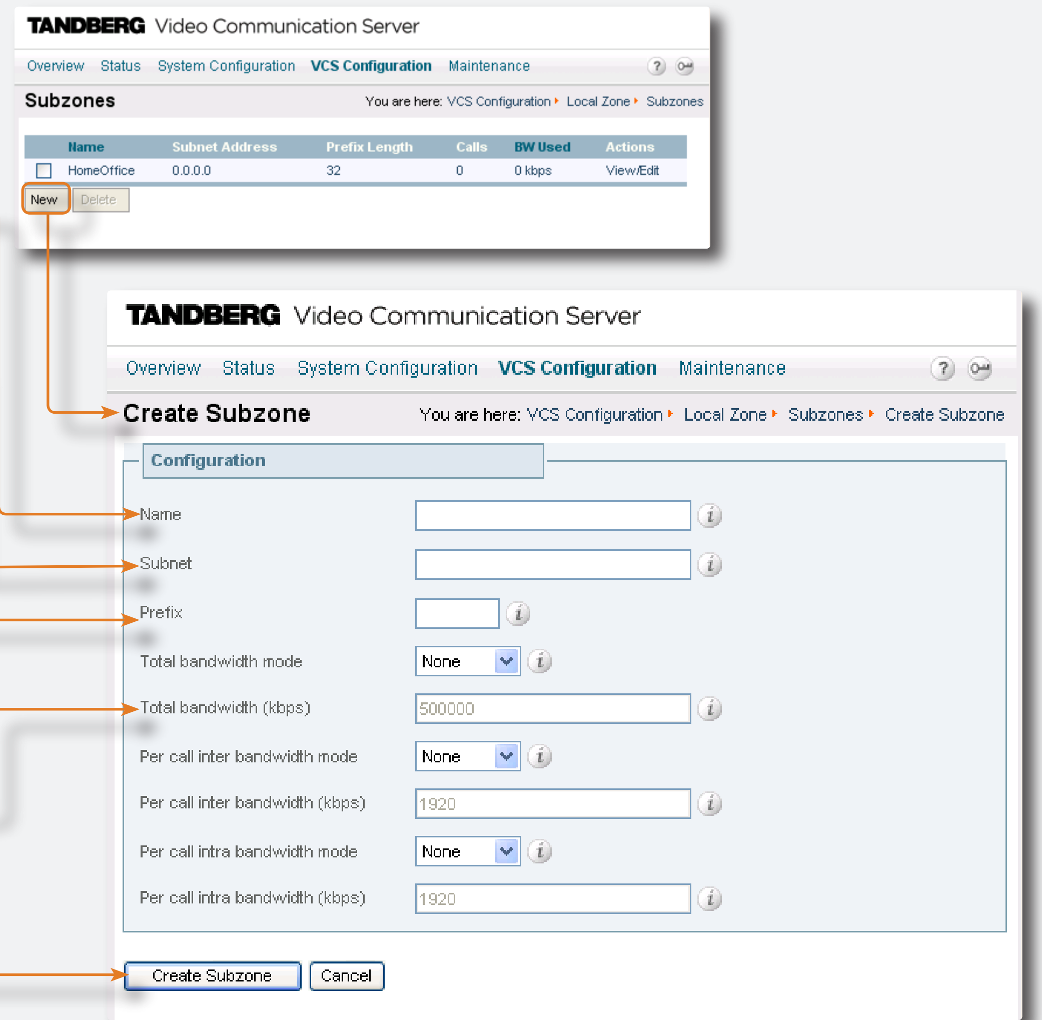
For example:
255.255.0.0 is equivalent to a prefix length of 16
255.255.255.0 is equivalent to a prefix length of 24

Bandwidth

See Applying Bandwidth Limitations to Subzones for a description of these fields.

Create Subzone

Click here to create the subzone and return to the subzones page.



Bandwidth Control

Configuring a Subzone

To configure a subzone:

- *VCS Configuration > Local Zone > Subzones*.
  You will be taken to the Subzones page.
  Click on the subzone you wish to configure.
  You will be taken to the Edit Subzone page.
- `xConfiguration Zones LocalZone SubZone`

Name

Enter the name you wish to assign to the subzone. You will refer to this name when creating Links and Pipes.

Subnet 1

Enter the subnet IP Address and Prefix, This will define the range of IP addresses that will belong to this subzone.

Subnet 2 - 5

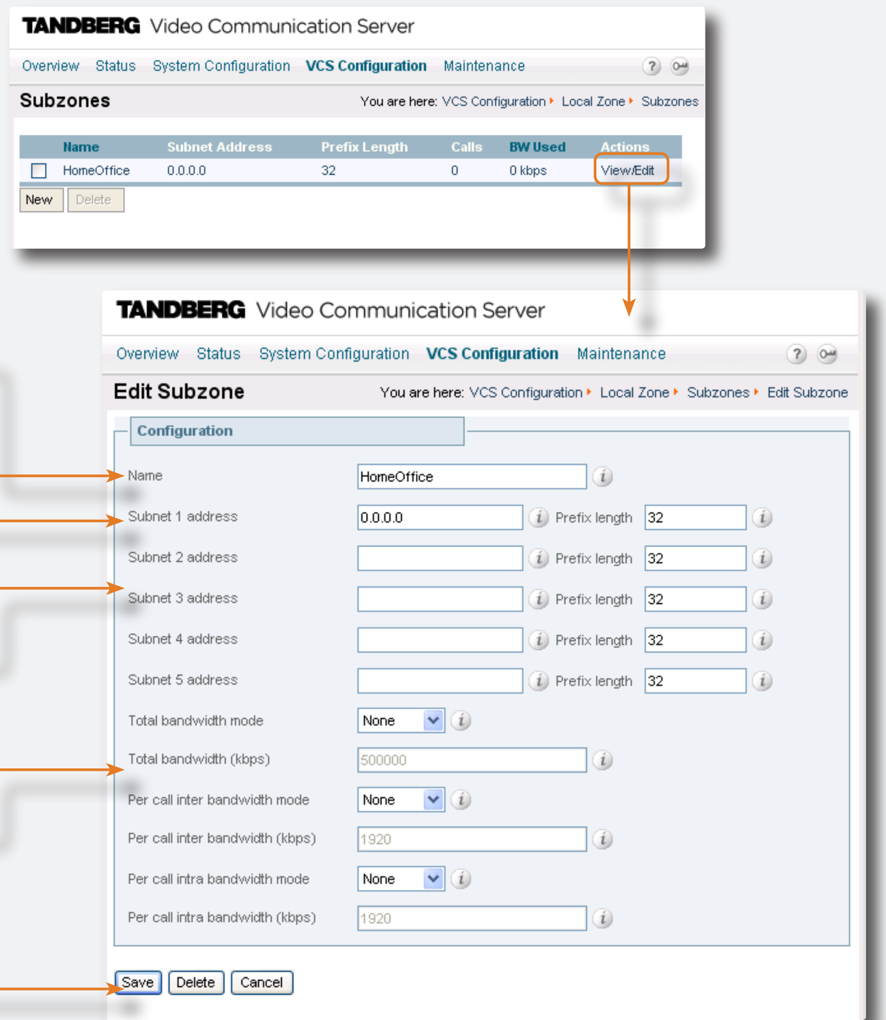
Use these fields to define up to 4 further subnets for this Subzone.

Bandwidth

See Applying Bandwidth Limitations to Subzones for a description of these fields.

Save

Click here to save your changes.



Bandwidth Control

Applying Bandwidth Limitations to Subzones

Types of Limitations

You can apply bandwidth limits to the Default Subzone, Traversal Subzone and all manually configured subzones. The types of limitations you can apply vary depending on the type of subzone, as follows:

Limitation	Description	Can be applied to
Total	Limits the total concurrent bandwidth being used by all endpoints in the subzone at any one time.	• Default Subzone • Traversal Subzone • Manually configured subzones
Per call intra	Limits the bandwidth of any individual call between two endpoints within the subzone.	• Default Subzone • Manually configured subzones
Per call inter	Limits the bandwidth of any individual call between an endpoint in the subzone, and an endpoint in another subzone or zone.	• Default Subzone • Traversal Subzone • Manually configured subzones

For all these settings, a bandwidth mode of:

- None will mean that no bandwidth is allocated and therefore no calls can be made.
- Limited will mean that limits are applied. You must also enter a value in the corresponding bandwidth (kbps) field.
- Unlimited will mean that no restrictions will be applied to the amount of bandwidth being used.

How Different Bandwidth Limitations are Managed

In situations where there are differing bandwidth limitations applied to the same link, the lower limit will always be the one used when routing the call and taking bandwidth limitations into account.

For example, Subzone A may have a per call inter bandwidth of 128. This means that any calls between Subzone A and any other subzone or zone will be limited to 128kbps. However, Subzone A also has a link configured between it and Subzone B. This link uses a pipe with a limit of 512kbps. In this situation, the lower limit of 128kbps will apply to calls between the two, regardless of the larger capacity of the pipe.

In the reverse situation, where Subzone A has a per call inter bandwidth limit of 512kbps and a link to Subzone B with a pipe of 128, any calls between the two subzones will still be limited to 128kbps.

Use subzone bandwidth limits if you want to configure the bandwidth available between one specific subzone and all other subzones or zones.

Use Pipes if you want to configure the bandwidth available between one specific subzone and another specific subzone or zone.

If your bandwidth configuration is such that multiple types of bandwidth restrictions are placed on a call (for example, if there are both subzone bandwidth limits and pipe limits), the lowest limit will always apply to that call.

A non-traversal call between two endpoints within the same subzone would consume the amount of bandwidth of that call. A traversal call between two endpoints within the same subzone must, like any other traversal call, pass through the Traversal Subzone. This means that such calls will consume from the originating subzone's total concurrent allocation twice the bandwidth of the call – once for the call from the subzone to the Traversal Subzone, and again for the call from the Traversal Subzone back to the originating subzone.

Calls passing through the Traversal Subzone consume an amount of bandwidth within the subzone equal to that of the call.

Bandwidth Control

About Pipes

It is possible to control the amount of bandwidth used on calls between specific subzones and zones. The limits can be applied to the total concurrent bandwidth used at any one time, or to the bandwidth used by any individual call.

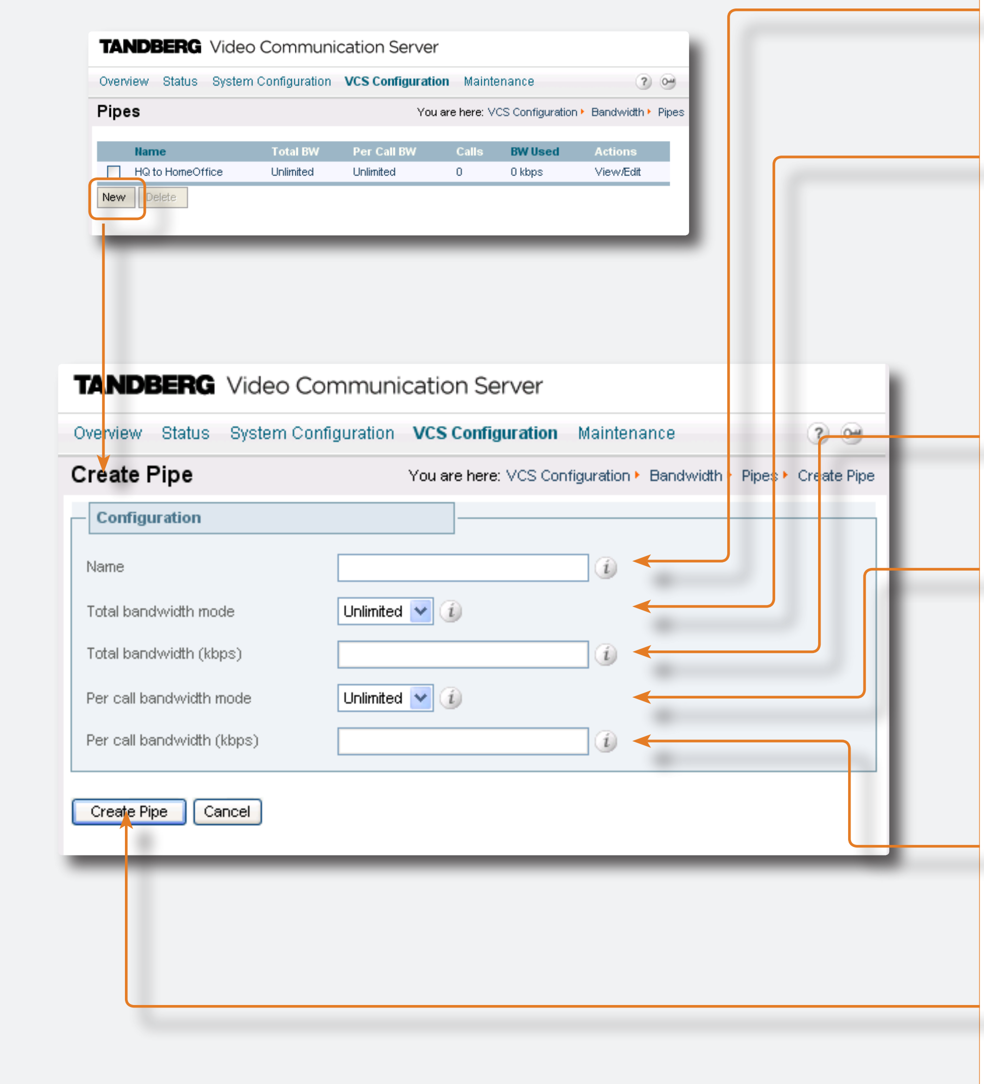
To apply these limits, you create a pipe and configure it with the required bandwidth limitations. You then assign the pipe to a link. Calls using the link will then have those bandwidth limitations applied to them.

Creating a new pipe

To create a pipe:

- *VCS Configuration > Bandwidth > Pipes*.
  You will be taken to the Pipes page.
  Select New.
  You will be taken to the Create Pipe page.
- xCommand PipeAdd

Creating Pipes



Name

Enter the name you wish to give to this pipe. You will refer to this name when creating links.

Total bandwidth mode

Determines whether there is a limit on the total concurrent bandwidth of this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

None: there is no bandwidth available.

Total bandwidth (kbps)

Sets the limit on the total concurrent bandwidth of this pipe.

Per call bandwidth mode

Determines whether there is a limit on the bandwidth of individual calls via this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

None: there is no bandwidth available.

Per call bandwidth (kbps)

Sets the limit on the bandwidth of individual calls via this pipe.

Create Pipe

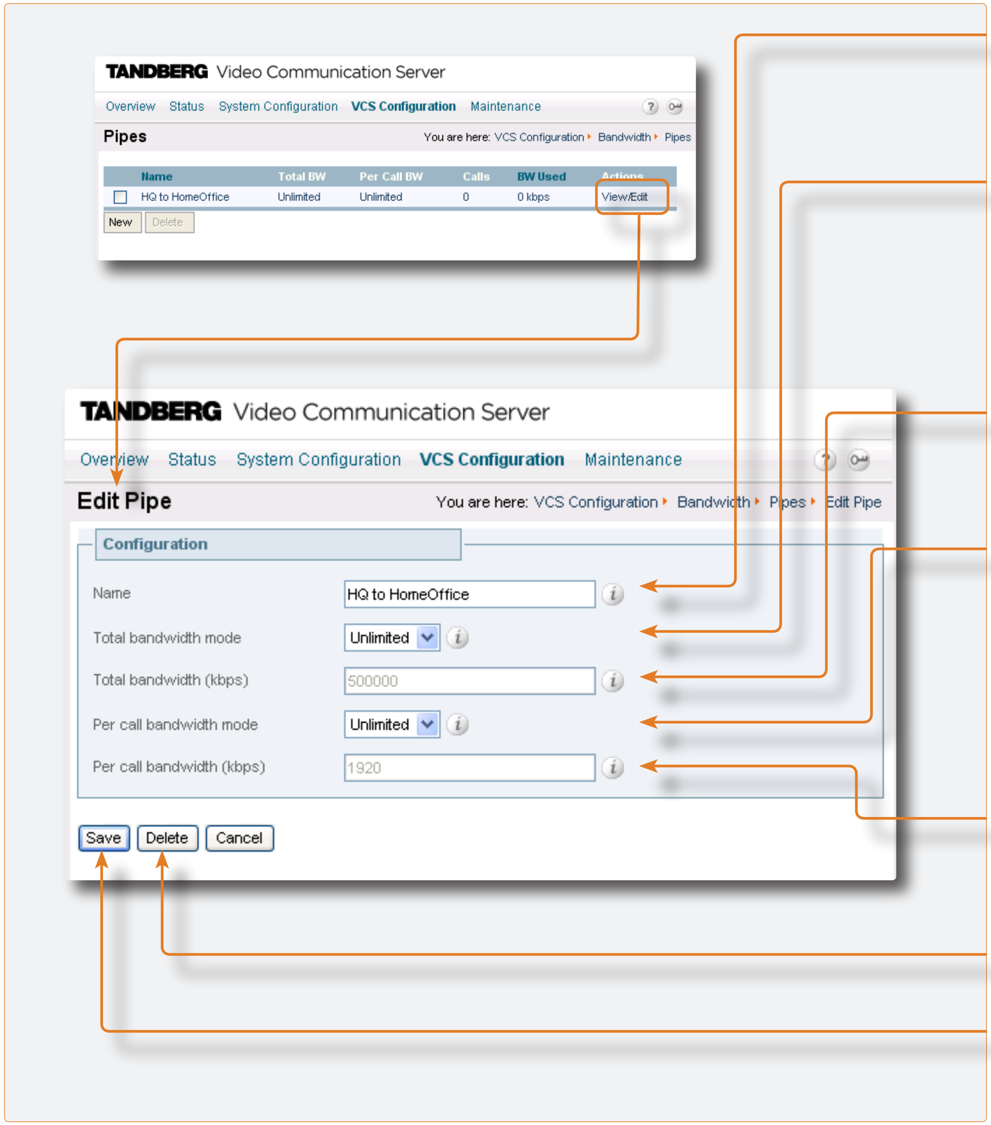
Click here to create the pipe and return to the Pipes page.

Editing Pipes

Editing an Existing Pipe

To configure details of a pipe:

- *VCS Configuration > Bandwidth > Pipes*
  You will be taken to the Pipes page.
  Click on the pipe you wish to configure.
  You will be taken to the Edit Pipe page.
- `xConfiguration Bandwidth Pipe`



Name

Enter the name you wish to give to this pipe. You will refer to this name when creating links.

Total bandwidth mode

Determines whether there is a limit on the total concurrent bandwidth of this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

None: there is no bandwidth available.

Total bandwidth (kbps)

Sets the limit on the total concurrent bandwidth of this pipe.

Per call bandwidth mode

Determines whether there is a limit on the bandwidth of individual calls via this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

None: there is no bandwidth available.

Per call bandwidth (kbps)

Sets the limit on the bandwidth of individual calls via this pipe.

Delete

Click here to delete the pipe.

Save

Click here to save the changes.

Bandwidth Control

About Links

Subzones are connected to other subzones and zones via links. For a call to take place, the endpoints involved must each reside in subzones or zones that have a link between them. The link does not need to be direct; the two endpoints may be linked via one or more intermediary subzones.

Links are used to calculate how a call is routed over the network and therefore which zones and subzones are involved and how much bandwidth is available. If multiple routes are possible, your VCS will perform the bandwidth calculations using the one with the fewest links.

Creating a New Link

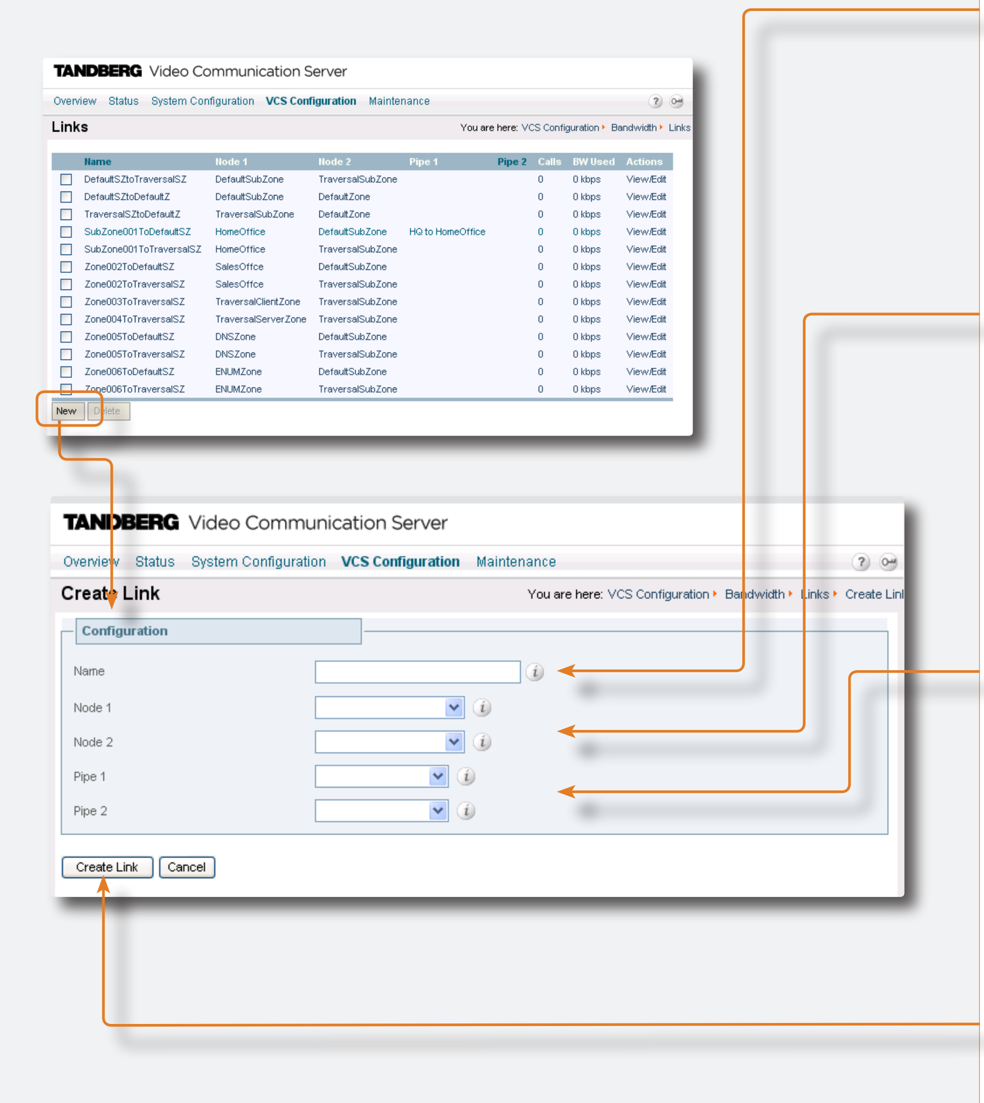
To create a new link:

- *VCS Configuration > Bandwidth > Links*.
  You will be taken to the Links page.
  Click New.
  You will be taken to the Create Link page.
- `xCommand LinkAdd`

Default Links

If a subzone has no links configured, then endpoints within the subzone will only be able to call other endpoints within the same subzone. For this reason, when a subzone is created, it is automatically given certain links. See Default Links for more information.

Creating Links



Name

Enter the name you wish to assign to this link.

Node 1, Node 2

Select the names of the two subzones, or the subzone and zone between which you wish to create a link.

Pipe 1, Pipe 2

If you wish to apply bandwidth limitations to this link, select the pipe(s) to be applied.

For more information, see Applying Pipes to Links.

Create Link

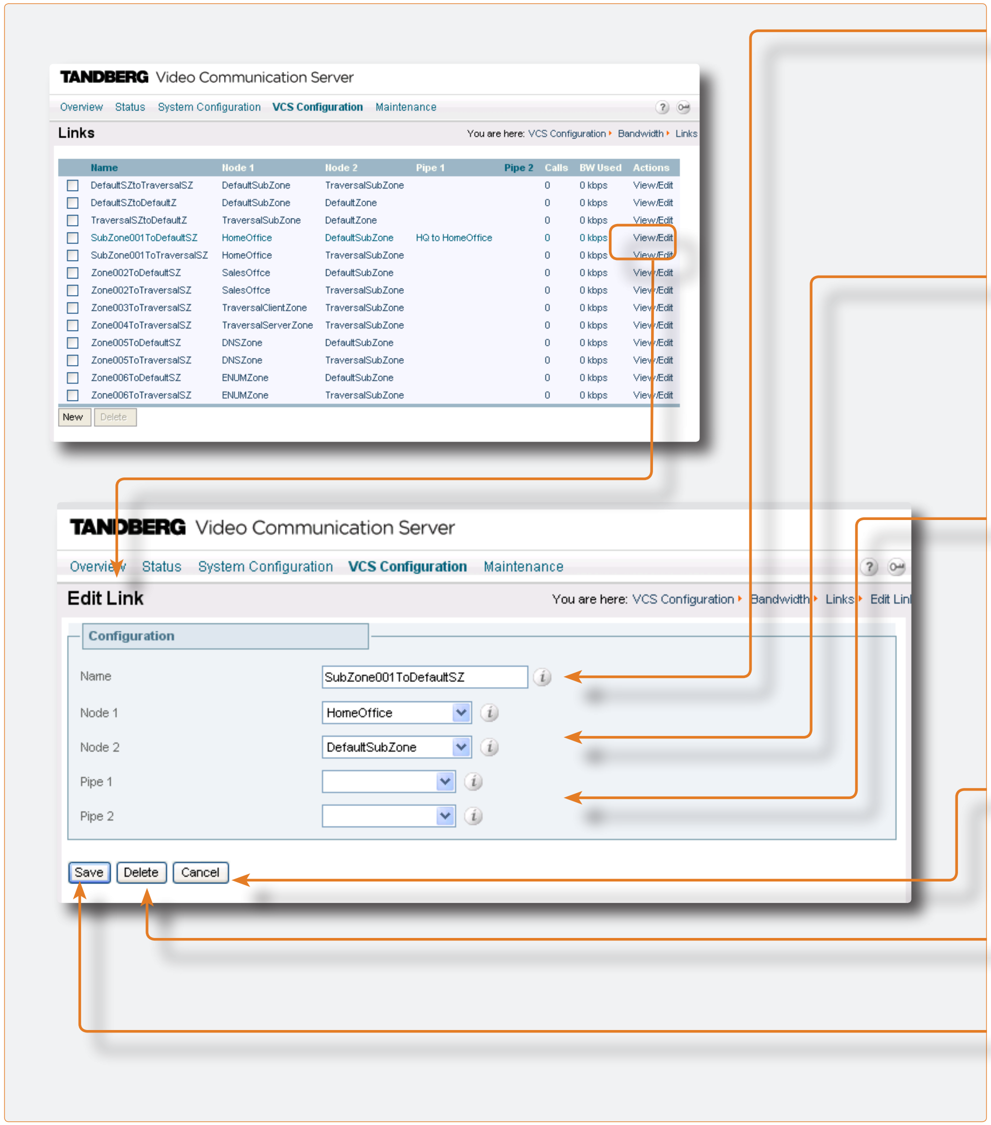
Click here to create the link and return to the Links page.

Editing Links

Editing Links

To edit a link:

- *VCS Configuration > Bandwidth > Links*.
  You will be taken to the Links page.
  Click View/Edit.
  You will be taken to the Edit Link page.
- `xConfiguration Bandwidth Link`



Name

Enter the name you wish to assign to this link.

Node 1, Node 2

Select the names of the two subzones, or the subzone and zone between which you wish to create a link.

Pipe 1, Pipe 2

If you wish to apply bandwidth limitations to this link, select the pipe(s) to be applied.

For more information, see Applying Pipes to Links.

Cancel

Click here to return to the Links page without saving your changes.

Delete

Click here to delete the link.

Save

Click here to save your changes.

Bandwidth Control

Applying Pipes to Links

Pipes are used to restrict the bandwidth of a link. When a pipe is applied to a link, it will restrict the bandwidth of calls made between the two nodes of the link - the restrictions will apply to calls in either direction.

Normally a single pipe would be applied to a single link. However, one or more pipes may be applied to one or more links, depending on how you wish to model your network.

One Pipe, One Link

Applying a single pipe to a single link is useful when you wish to apply specific limits to calls between a subzone and another specific subzone or zone.

One Pipe, Two or More Links

Each pipe may be applied to multiple links. This is used to model the situation where one site communicates with several other sites over the same broadband connection to the Internet. A pipe should be configured to represent the broadband connection, and then applied to all the links. This will allow you to configure the bandwidth options for calls in and out of that site.

Two Pipes, One Link

Each link may have up to two pipes associated with it. This is used to model the situation where the two nodes of a link are not directly connected, for example two sites that each have their own broadband connection to the Internet. Each connection should have its own pipe, meaning that a link between the two nodes should be subject to the bandwidth restrictions of both pipes.

Default Links

About Default Links

If a subzone has no links configured, then endpoints within the subzone will only be able to call other endpoints within the same subzone. For this reason, the VCS comes shipped with a set of pre-configured links and will also automatically create new links each time you create a new subzone.

Pre-Configured Links

The VCS is shipped with the Default Subzone, Traversal Subzone and Default Zone already created, and with links pre-configured between the three. You may delete or amend these default links if you need to model restrictions of your network.

If any of these links have been deleted, they may all be automatically restored via:

- `xCommand DefaultLinksAdd`

To restore these links via the web interface, you must do so manually. See Creating Links for instructions on how to do this.

Automatically Created Links

Whenever a new subzone or zone is created, links are automatically created as follows:

New zone/subzone type	Default links are created to...
Subzone	Default Subzone and Traversal Subzone
Neighbor zone	Default Subzone and Traversal Subzone
DNS Zone	Default Subzone and Traversal Subzone
ENUM Zone	Default Subzone and Traversal Subzone
Traversal Client Zone	Traversal Subzone
Traversal Server Zone	Traversal Subzone

You can edit any of these default links in the same way you would edit manually configured links. See Editing Links for more information.

Calls will fail if links are not configured correctly.

Bandwidth Control

Default Call Bandwidth, Insufficient Bandwidth and Downspeeding

About the Default Call Bandwidth

Usually, when a call is initiated the endpoint will include in the request the amount of bandwidth it wishes to use. For those cases where the endpoint has not specified the bandwidth, you can set the VCS to apply a default bandwidth value.

Configuring the Default Call Bandwidth and Downspeeding

The default call bandwidth and downspeeding behavior are configured via:

- *VCS Configuration > Bandwidth > Configuration*.
  You will be taken to the Bandwidth Configuration page.
- `xConfiguration Bandwidth Default`
- `xConfiguration Bandwidth Downspeed`

About Downspeeding

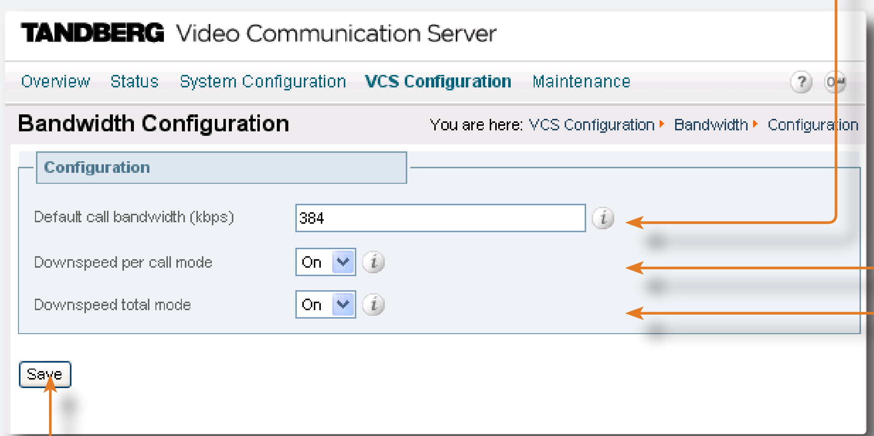
If bandwidth control is in use, there may be situations when there is insufficient bandwidth available to place a call at the requested rate. By default (and assuming that there is *some* bandwidth still available) the VCS will still attempt to connect the call, but at a reduced bandwidth – this is known as downspeeding.

You can turn off downspeeding, in which case if there is insufficient bandwidth to place the call at the originally requested rate, the call will not be placed at all. In this situation users will get one of the following messages, depending on the message that initiated the search:

- `Exceeds Call Capacity`
- `Gatekeeper Resources Unavailable`

Downspeeding can be configured so that it is applied in either or both of the following scenarios:

- when the requested bandwidth for the call exceeds the lowest per-call limit for the subzone or pipe(s)
- when placing the call at the requested bandwidth would mean that the total bandwidth limits for that subzone or pipe(s) would be exceeded.



Default call bandwidth (kbps)

Enter the bandwidth value to be used for calls for which no bandwidth value has been specified.

This value cannot be blank. The default value is 384 kbps.

Downspeed per call mode

Determines what will happen if the per-call bandwidth restrictions on a subzone or pipe mean that there is insufficient bandwidth available to place a call at the requested rate.

On: the call will be downspeeded.

Off: the call will not be placed.

Downspeed total mode

Determines what will happen if the total bandwidth restrictions on a subzone or pipe mean that there is insufficient bandwidth available to place a call at the requested rate.

On: the call will be downspeeded.

Off: the call will not be placed.

Save

Click here to save your changes

Bandwidth Control Examples

Example Without a Firewall

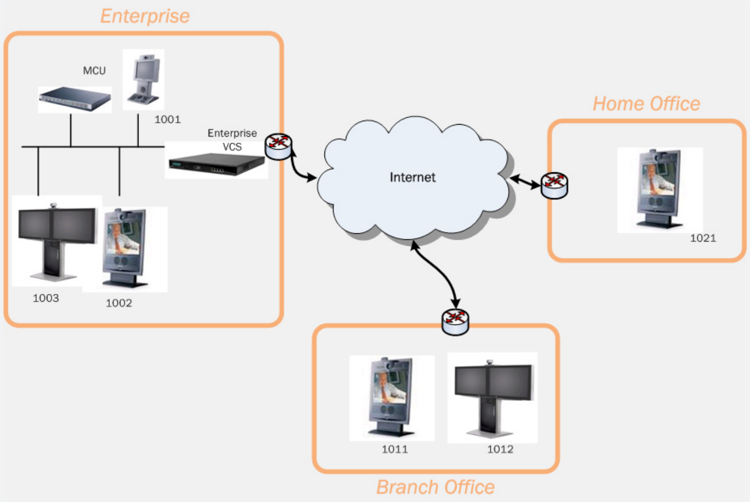
An example deployment is shown opposite.

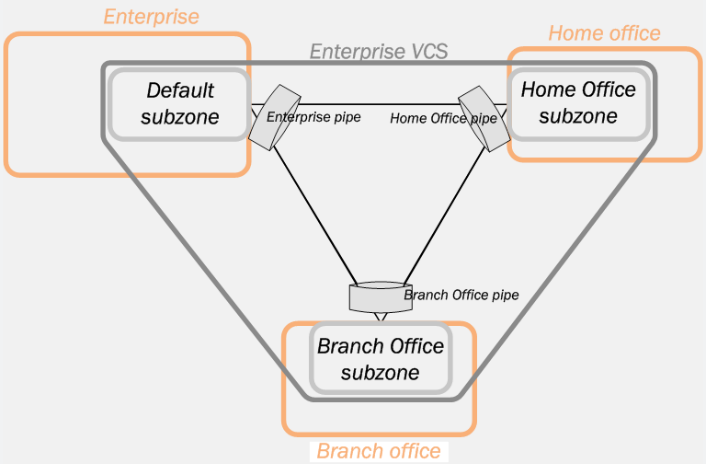
Each of the three offices (Enterprise, Home and Branch) is represented as a separate subzone on the VCS, with bandwidth configured according to local policy.

The enterprise's leased line connection to the Internet, and the DSL connections to the remote offices, are modeled as separate pipes.

There are no firewalls involved in this scenario, so we can configure direct links between each of the offices. Each link is then assigned two pipes, representing the Internet connections of the offices at each end of the link.

In this scenario, a call placed between the Home Office and Branch Office will consume bandwidth from the Home and Branch subzones and on the Home and Branch pipes. The Enterprise's bandwidth budget will be unaffected by the call.





Bandwidth Control

Bandwidth Control Examples

Example With a Firewall

If we modify the previous example deployment to include firewalls between the offices, we can use TANDBERG's Expressway™ firewall traversal solution to maintain connectivity. We do this by adding a VCS Border Controller outside the firewalls on the public internet, which will work in conjunction with the Enterprise VCS and Home and Branch office endpoints to traverse the firewalls.

This example, the endpoints in the enterprise register with the Enterprise VCS, whilst those in the Branch and Home offices register with the VCS Border Controller.

The introduction of the firewalls means that there is no longer any direct connectivity between the Branch and Home offices. All traffic must be routed through the VCS Border Controller. This is shown by the absence of a link between the Home and Branch subzones.

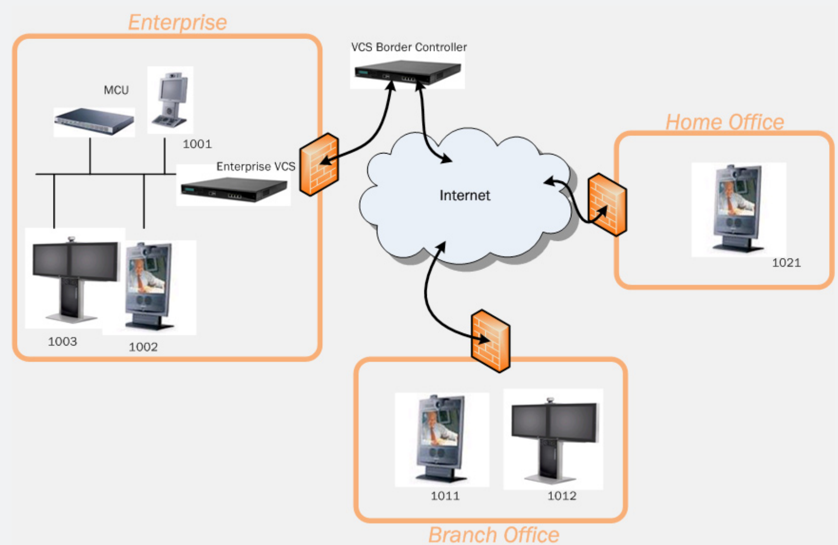
VCS Border Controller Subzone Configuration

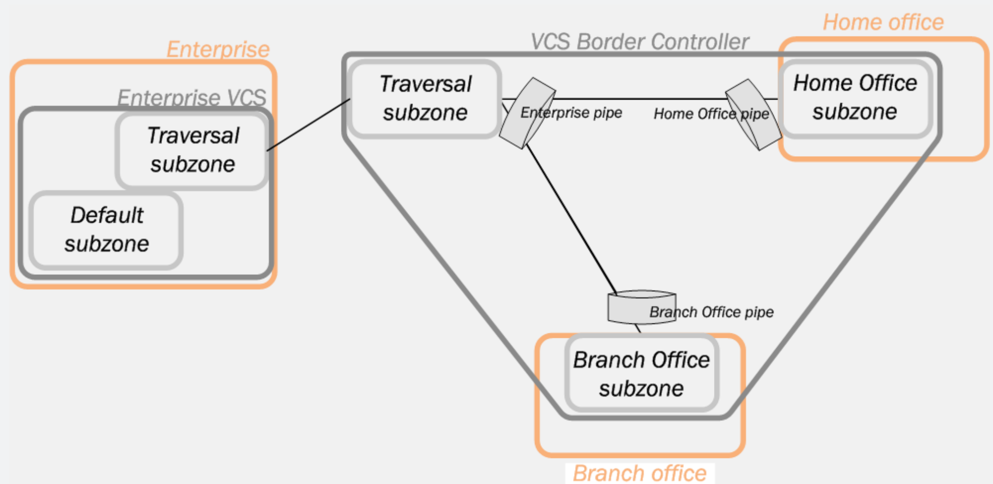
The VCS Border Controller has subzones configured for the Home Office and Branch Office. These are linked to the VCS Border Controller's Traversal Subzone, with pipes placed on each link. All calls from the VCS Border Controller to the Enterprise VCS must go through the Traversal Subzone and will consume bandwidth from this Subzone. Note also that calls from the Home Office to the Branch Office must also go through the Traversal Subzone, and will also consume bandwidth from this Subzone as well as the Home and Branch subzones and Home Office, Branch office and Enterprise pipes.

In this example we have assumed that there is no bottleneck on the link between the VCS Border Controller and the Enterprise network, so have not placed a pipe on this link. If you want to limit the amount of traffic flowing through your firewall, you could provision a pipe on this link.

Enterprise VCS Subzone Configuration

Because the Enterprise VCS is only managing endpoints on the LAN, its configuration is simpler. All of the endpoints in the enterprise are assigned to the Default Subzone. This is linked to the Traversal Subzone, through which all calls leaving the Enterprise must pass.





Upgrading Software

About Upgrading the VCS Software

It is possible to install new releases of the VCS software on your existing hardware. Software upgrade can be done in one of two ways:

- using secure copy (SCP/PSCP).
- using the web interface (HTTP/HTTPS)

This section describes how both of these methods are used to perform upgrades.

Prerequisites

The upgrade requires you to have:

- a valid Release key
- a software image file

Contact your TANDBERG representative for more information on how to obtain these.

Backing up the Existing Configuration Before Upgrading

The existing configuration will be restored after performing an upgrade. However, we recommend that you make a backup of the existing configuration before performing the upgrade.

To do this:

1. Use the command line interface to log on to the VCS.
2. Issue the command `xConfiguration`.
3. Save the resulting output to a file, using cut-and-paste or some other means provided by your terminal emulator.

To restore your configuration:

1. Remove the `*c` from in front of each command.
2. Paste this information back in to the command line interface.

Upgrading Using SCP/PSCP

To upgrade using SCP or PSCP (part of the PuTTY free Telnet/SSH package) you will need to transfer two files to the VCS:

- a text file containing just the 16-character Release Key
- the file containing the software image.

To upgrade using SCP or PSCP:

1. Ensure the VCS is turned on and available on IP.
2. Upload the release key file using SCP/PSCP to the `/tmp` folder on the system e.g.
   `scp release-key root@10.0.0.1:/tmp/release-key` or
   `pscp release-key root@10.0.0.1:/tmp/release-key`
3. Enter password when prompted.
4. Copy the software image using SCP/PSCP. The target name must be `/tmp/tandberg-image.tar.gz`, e.g.
   `scp s42100x11.tar.gz root@10.0.0.1:/tmp/tandberg-image.tar.gz` or
   `pscp s42100x11.tar.gz root@10.0.0.1:/tmp/tandbergimage.tar.gz`
5. Enter password when prompted.
6. Wait until the software has installed completely. This should not take more than two minutes.
7. Reboot the system.

After about four minutes the system will be ready to use.

⚠ You must name the files exactly as described above.

⚠ You must transfer the Release Key file before transferring the software image.

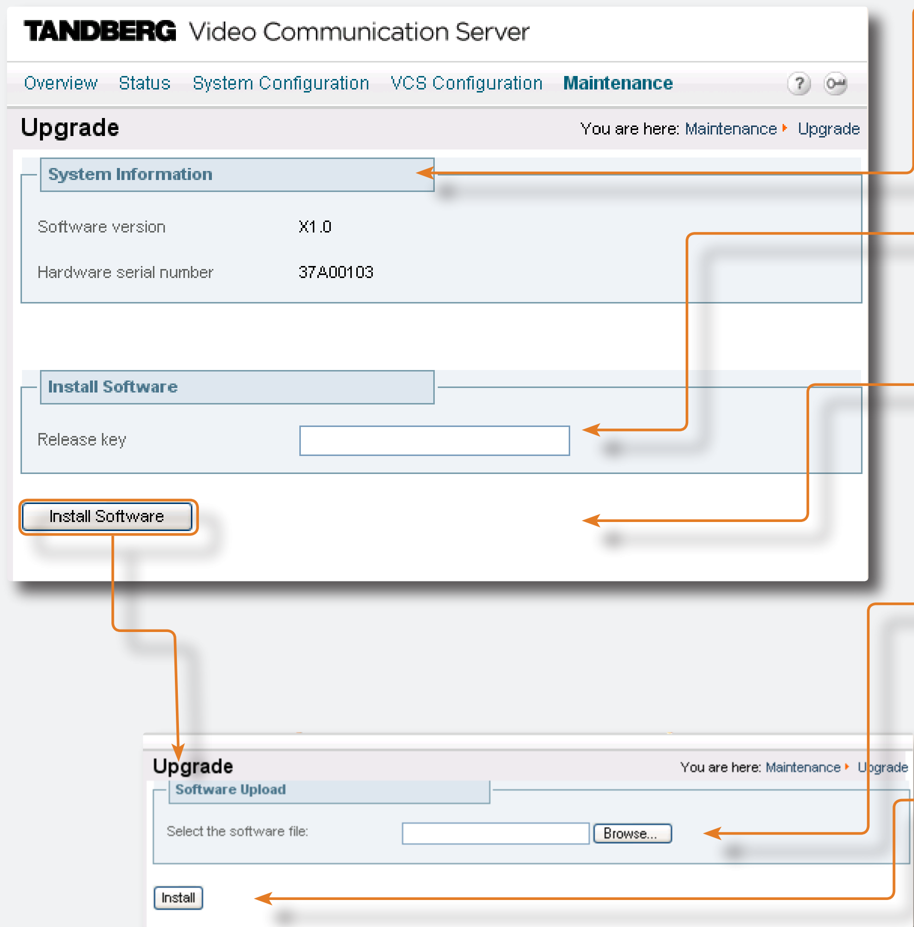
Upgrading

Upgrading via the Web Interface

To upgrade your software via the web interface:

- *Maintenance > Upgrade*.
  You will be taken to the Upgrade page.

Before you start the upgrade, ensure that the software image file has been saved in a network location that can be accessed via the web interface. Also ensure that you have the 16-character Release Key readily available.



System Information

This section tells you about the software and hardware that currently make up your system.

Release key

Enter the 16-character Release Key that has been provided to you.

Install Software

Click Install Software. You will be taken to a new page.

Select the software file

Enter the path of the software image file, or click Browse to locate it on the network.

Install

Click here to upload the image file.

Option Keys

About Adding Extra Options

The following VCS features can be added to your existing system by installing the appropriate options:

- Border Controller functionality
- user policy
- H.323 to SIP Interworking gateway
- the number of traversal calls allowed
- the number of non-traversal calls allowed
- the number of registrations allowed

To add any of these extra options, you need to obtain a valid Option Key and install it on your system. Contact your TANDBERG representative for more information on how to obtain Option Keys.

Options can be installed in either of two ways:

- via the CLI.
- via the web interface.

This section describes both methods.

Adding Options via the CLI

To return the indexes of all the Option Keys that are already installed on your system:

- `xStatus Options`

To add a new Option Key to your system:

- `xConfiguration Option [1..64] Key: <S: 0, 90>`

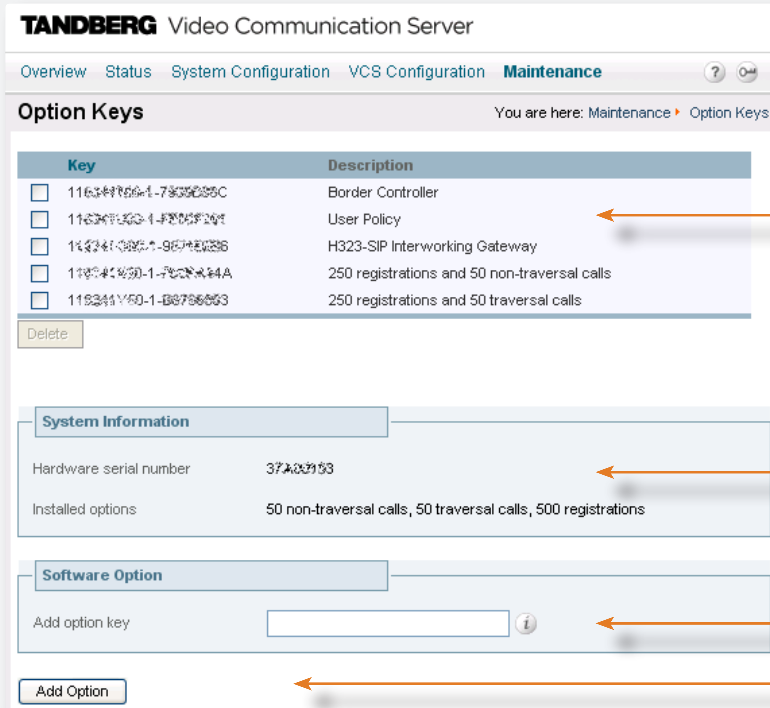
When using the CLI to add an extra option key, you can use any unused option index. If you chose an existing option index, that option will be overwritten and the extra functionality will no longer exist.

Option Keys

Adding Options via the Web Interface

To add options via the web interface:

- *Maintenance > Option Keys*.
  You will be taken to the Option Keys page.



This section lists the keys that are already installed on your system along with a description of the options they provide.

System Information

This section tells you about the hardware and options that currently make up your system.

Add option key

Enter the 20-character Option Key that has been provided to you for the option you wish to add.

Add Option

Click Add Option.

Maintenance

Security

About Security

For extra security, you may wish to have the VCS communicate with other systems (e.g. servers such as LDAP servers or clients such as SIP endpoints) using TLS encryption.

For this to work successfully in a connection between a client and server:

- the server must have a certificate installed that verifies its identity. This certificate must be signed by a Certificate Authority (CA).
- the client must trust the CA that signed the certificate used by the server.

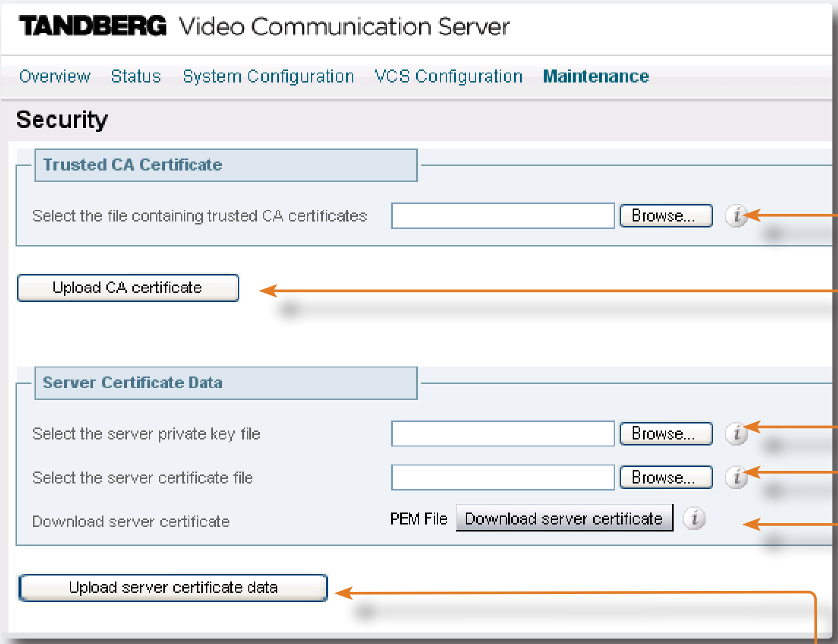
The VCS allows you to install appropriate files so that it can act as either a client or a server in connections using TLS.

Enabling Security

The files that enable secure connections over TLS are installed via the web interface. They cannot be installed using the CLI.

To enable security using the web interface:

- *Maintenance > Security*.
  You will be taken to the Security page.



Select the file containing trusted CA...

Allows you to upload a PEM file that identifies the list of Certificate Authorities trusted by the VCS. The VCS will only accept certificates signed by a CA on this list. If you are connecting to an LDAP database using TLS encryption, the certificate used by the LDAP database must be signed by a CA on this list.

Upload CA certificate

Click here once you have selected the file to upload it.

Select the server private key file

Allows you to upload a PEM file that identifies the private key used to encrypt the server certificate used by the VCS. This private key must not be password protected.

Select the server certificate file

Allows you to uploads PEM file that contains the server certificate used for HTTPS connections to the VCS from user or administrator web browsers, and by SIP endpoints or servers connecting to the VCS over TLS.

Download server certificate

Provides you with the PEM file containing the certificate used by the VCS to identify itself to SIP and HTTPS clients when communicating over SSL/TLS.

Upload server certificate data

Click here once you have selected the files to upload them.

Passwords

Changing the Administrator Password

To change the password used to log in to the VCS:

- *Maintenance > Passwords*.
  You will be taken to the Passwords page.

You must restart the system for changes to take effect.

New password

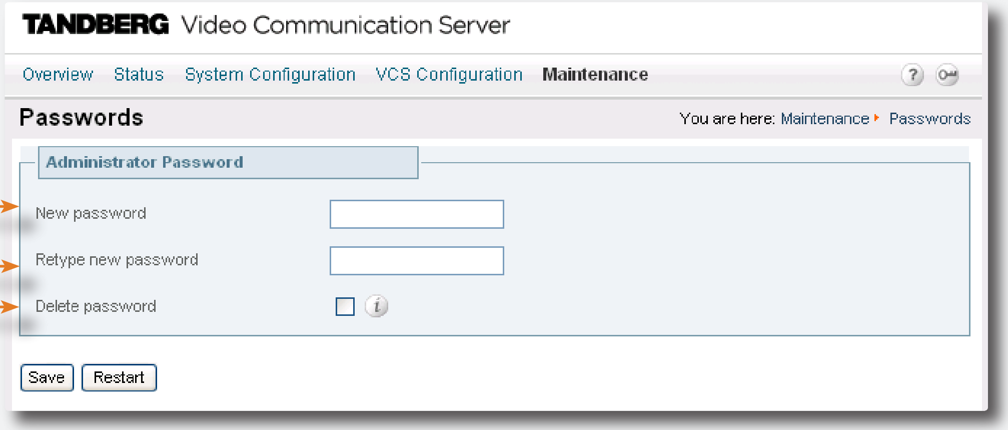
Enter your new password here.

Retype new password

Retype your new password here.

Delete password

Click here to reset the Administrator Password to a blank field.



System Snapshot

About the System Snapshot

The system snapshot is used for diagnostic purposes. It is a file that can be sent to your system support representative at their request to assist them in troubleshooting issues you may be experiencing.

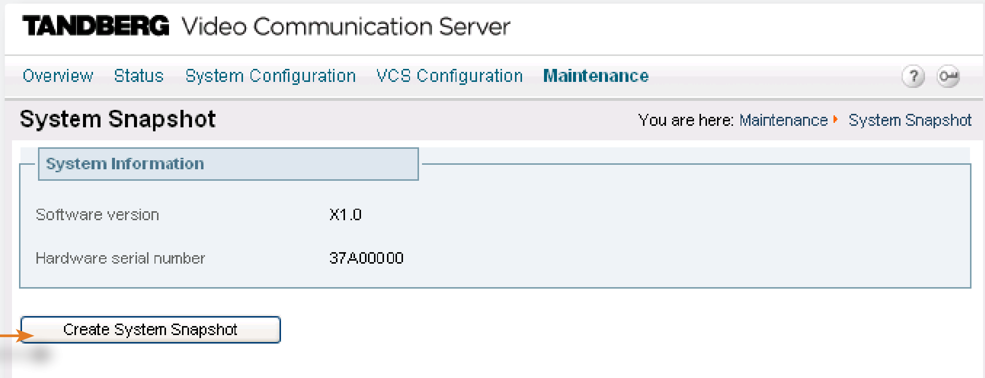
Creating a System Snapshot

To create a system snapshot file:

- *Maintenance > System Snapshot*.
  You will be taken to the System Snapshot page.

  Click on the Create System Snapshot button.

Save the resulting file to an appropriate location.



Restarting

About Restarting

Some configuration changes will require a restart of the system to take effect. There will be a Restart button at the bottom of any web pages that include such options. If you do not restart the system after making these changes, you will receive a warning telling you the system needs to be restarted.

Restarting will cause any active calls to be terminated.

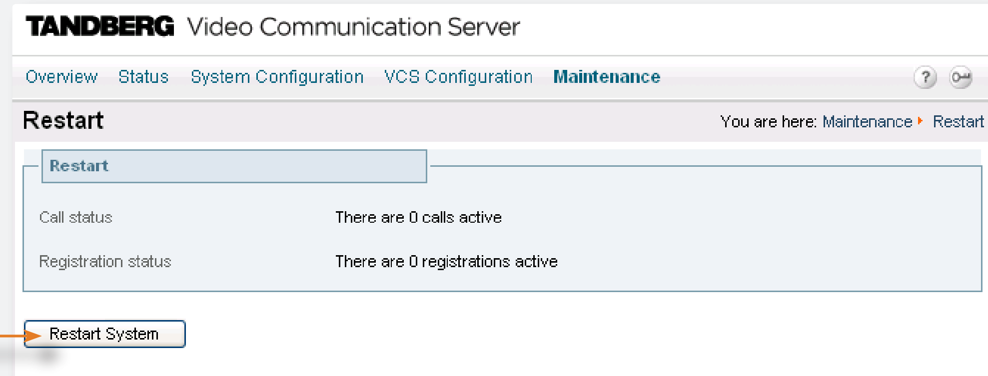
There are two ways to restart the system:

- *Maintenance > Restart*.
  You will be taken to the Restart page.
- `xCommand Boot`

Do not restart the system while the red ALM LED on the front of the box is flashing.

Restart System

Click here to restart the system.



Shutting Down

About Shutting Down

The system must be shut down before it is unplugged.

Once the system has been shut down, the only way it can be restarted is by pressing the soft power button on the unit itself. You must therefore have physical access to the unit if you wish to be able to restart it after shut down.

Shutting down will cause any active calls to be terminated.

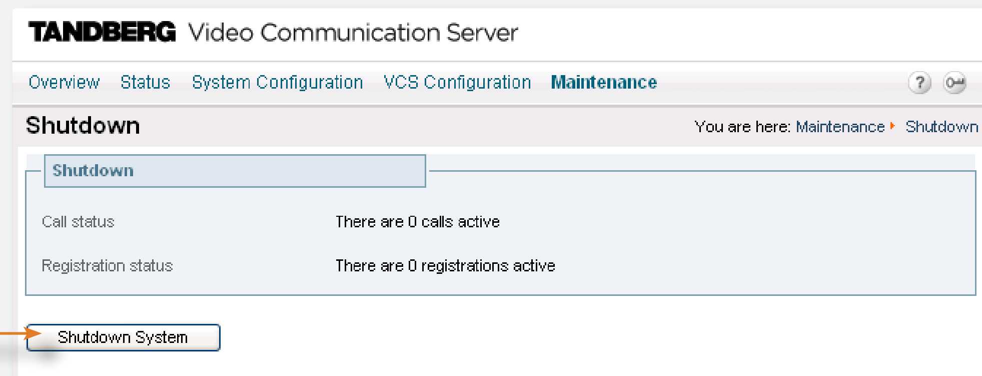
To shut down the system:

- *Maintenance > Shutdown*.
  You will be taken to the Shutdown page.

Do not shutdown the system while the red ALM LED on the front of the box is flashing.

Shutdown System

Click here to shutdown the system.



Administration	**HTTP**	**Mode: <On/Off>** Determines whether HTTP calls will be redirected to the HTTPS port. On: calls will be redirected to HTTPS. Off: no HTTP access will be available.
	HTTPS	**Mode: <On/Off>** Determines whether the VCS can be accessed via HTTPS. This must be On to enable both web interface and TMS access. On: HTTPS access is enabled. Off: HTTPS access is disabled.
	SSH	**Mode: <On/Off>** Determines whether the VCS can be accessed via SSH and SCP. On: SSH/SCP access is enabled. Off: SSH/SCP access is disabled.
	Telnet	**Mode: <On/Off>** Determines whether the VCS can be accessed via Telnet. On: Telnet access is enabled. Off: Telnet access is disabled.
	TimeOut: <0..10000> Sets the number of minutes that an administration session (HTTPS, Telnet or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off.	
Alternates	**Alternate [1..5]**	**Address: <S: 0, 128>** Specifies the IP address of an alternate VCS. Up to 5 alternates may be configured. When the VCS receives a Location Request, all alternates will also be queried.
Authentication	**Credential [1..2500]**	**Name: <S: 0, 255>** Defines the name for this entry in the local authentication database.
		Password: <S: 0, 50> Defines the password for this entry in the local authentication database.
	Database: <LocalDatabase/LDAPDatabase> Selects the database to be used for the storage of password information for authentication. LocalDatabase: the local database will be used. LDAPDatabase: a remote LDAP repository will be used.	

Authentication cont...	**LDAP**		**AliasOrigin: <LDAP/Endpoint/Combined>** Determines which aliases (i.e. from the endpoint or the database) should be used to register the endpoint. LDAP: the alias(es) presented by the endpoint will be used as long as they are listed in the LDAP database for the endpoint's username. Endpoint: the alias(es) presented by the endpoint will be used; any in the LDAP database will be ignored. Combined: the alias(es) presented by the endpoint will be used in addition to any that are listed in the LDAP database for the endpoint's username.
			BaseDN: <S: 0, 255> Specifies the Distinguished Name to use when connecting to an LDAP server.
	Mode: <On/Off> Determines whether or not to enforce authentication for H.323 and SIP registrations. On: authentication is required. Off: authentication is not required.		
	Password: <S: 0, 50> **Specifies the password to be used by the VCS when authenticating with another system.**		
	UserName: <S: 0, 255> **Specifies the username to be used by the VCS when authenticating with another system.**		
Bandwidth	**Default: <64..2048>** **Sets the bandwidth (in kbps) to be used on calls managed by the VCS in cases where no bandwidth has been specified by the endpoint.**		
	Downspeed	**PerCall**	**Mode: <On/Off>** Determines whether or not the system will attempt to downspeed a call if there is insufficient per-call bandwidth available to fulfil the request. On: the system will attempt to place the call at a lower bandwidth. Off: the call will be rejected.
		Total	**Mode: <On/Off>** Determines whether or not the system will attempt to downspeed a call if there is insufficient total bandwidth available to fulfill the request. On: the system will attempt to place the call at a lower bandwidth. Off: the call will be rejected.

Command Reference - xConfiguration

Bandwidth cont...	Link [1..400]	Name: <S: 1, 50> Assigns a name to this link.		
		Node1	Name: <S: 0, 50> Specifies the first zone or subzone to which this link will be applied.	
		Node2	Name: <S: 0, 50> Specifies the second zone or subzone to which this link will be applied.	
		Pipe1	Name: <S: 0, 50> Specifies the first pipe to be associated with this link.	
		Pipe2	Name: <S: 0, 50> Specifies the second pipe to be associated with this link.	
	Pipe [1..100]	Bandwidth	PerCall	Mode: <None/Limited/Unlimited> Determines whether or not this pipe is limiting the bandwidth of individual calls. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
				Limit: <1..1000000> If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call.
			Total	Mode: <None/Limited/Unlimited> Determines whether or not this pipe is enforcing total bandwidth restrictions. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
				Limit: <1..1000000> If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe.
		Name: <S: 1, 50> Assigns a name to this pipe.		

Command Reference - xConfiguration

Call	**Services**			**CallsToUnknownIPAddresses: <Off/Direct/Indirect>** Determines the way in which the VCS will attempt to call systems which are not registered with it or one of its neighbors. Direct: Allows an endpoint to make a call to an unknown IP address without the VCS querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system. Indirect: Upon receiving a call to an unknown IP address, the VCS will query its neighbors for the remote address, relying on the response from the neighbor to allow the ability for the call to be completed; connecting through the routing rules as it would through the neighbor relationship. Off: This will not allow any endpoint registered directly to the VCS to call an IP address of any system not also registered directly to that VCS.
				Fallback Alias: <S: 0, 60> Specifies the alias to which incoming calls are placed for calls where the IP address or domain name of the VCS has been given but no callee alias has been specified.
Ethernet				**Speed: <Auto/10half/10full/100half/100full/1000full/None>** Sets the speed of the Ethernet link. Auto: the VCS will automatically determine the speed to be used. 10half: a speed of 10half will be used. 10full: a speed of 10full will be used. 100half: a speed of 100half will be used. 100full: a speed of 100full will be used. 1000full: a speed of 1000full will be used. None: the VCS will automatically determine the speed to be used. Note: You must restart the system for any changes to take effect.
ExternalManager				**Address: <S: 0, 128>** Sets the IP address or FQDN of the External Manager.
				Path: <S: 0, 255> Sets the URL of the External Manager.
H323	**Gatekeeper**	**AutoDiscovery**		**Mode: <On/Off>** Determines whether or not the VCS responds to gatekeeper discovery requests from endpoints. On: the VCS will respond to requests. Off: the VCS will not respond to requests.
		CallSignaling	**PortRange**	**Start: <1024..65534>** Specifies the lower port in the range to be used by calls once they are established.
				End: <1024..65534> Specifies the upper port in the rage to be used by calls once they are established.

Command Reference - xConfiguration

H323 cont...	**Gatekeeper cont...**	**CallSignaling cont...**	**TCP**	**Port: <1024..65534>** Specifies the port that listens for H.323 call signaling.
		CallTimeToLive: <60..65534> Specifies the interval (in seconds) at which the VCS polls the endpoints in a call to verify that they are still in the call.		
		Registration	**ConflictMode: <Reject/Overwrite>** Determines how the system will behave if an endpoint attempts to register an alias currently registered from another IP address. Reject: denies the registration. Overwrite: deletes the original registration and replaces it with the new registration.	
			UDP Port: <1024..65534> Specifies the port to be used for H.323 UDP registrations.	
		TimeToLive: <60..65534> Specifies the interval (in seconds) at which an H.323 endpoint must re-register with the VCS in order to confirm that it is still functioning.		
	Mode: <On/Off> Determines whether or not the VCS will provide H.323 gatekeeper functionality. On: the VCS will act as an H.323 gatekeeper. Off: the VCS will not act as an H.323 gatekeeper.			
Interworking	**Mode: <On/Off/RegisteredOnly>** Determines whether or not the VCS will act as a gateway between SIP and H.323 calls. Off: the VCS will not act as a SIP-H.323 gateway. RegisteredOnly: the VCS will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered. On: the VCS will act as SIP-H.323 gateway regardless of whether the endpoints are locally registered (you must have the appropriate option key enabled to use this feature).			
IP	**Address: <IPAddr>** Specifies the IPv4 address of the VCS. Note: You must restart the system for any changes to take effect.			
	DNS	**Domain**	**Name: <S: 0, 128>** Specifies the name to be appended to the host name before a query to the DNS server is executed. Used only when attempting to resolve a domain name which is not fully qualified for NTP, LDAP, External Manager and Log servers.	
		Server [1..5]	**Address: <S: 0, 39>** Sets the IP address of up to 5 DNS servers to be used when resolving domain names.	
	Gateway: <IPAddr> Specifies the IPv4 gateway of the VCS. Note: You must restart the system for any changes to take effect.			

IP cont...		**SubnetMask: <IPAddr>** Specifies the IPv4 subnet mask of the VCS. Note: You must restart the system for any changes to take effect.
	V6	**Address: <S: 0, 39>** Specifies the IPv6 address of the VCS. Note: You must restart the system for any changes to take effect.
		Gateway: <S: 0, 39> Specifies the IPv6 gateway of the VCS. Note: You must restart the system for any changes to take effect.
IPProtocol: <Both/IPv4/IPv6> Selects the IP protocol(s) supported by the VCS. Both: the VCS will support both IPv4 and IPv6. IPv4: the VCS will support IPv4 only. IPv6: the VCS will support IPv6 only. Note: You must restart the system for any changes to take effect.		
LDAP		**Encryption: <Off/TLS>** Sets the encryption to be used for the connection to the LDAP server. Off: no encryption is used. TLS: TLS encryption is used.
		Password: <S: 0, 128> Sets the password to be used when binding to the LDAP server.
	Server	**Address: <S: 0, 128>** Sets the IP address or FQDN of the LDAP server to be used when making LDAP queries.
		Port: <1..65534> Sets the IP port of the LDAP server to be used when making LDAP queries.
		UserDN: <S: 0, 255> Sets the user distinguished name to be used when binding to the LDAP server.
Log		**Level: <1..3>** Controls the granularity of event logging. 1 is the least verbose, 3 the most.
	Server	**Address: <S: 0, 128>** Specifies the IP address or FQDN of the server to which the log will be written.
NTP		**Address: <S: 0, 128>** Sets the IP address or FQDN of the NTP server to be used when synchronizing system time.

Command Reference - xConfiguration

Option [1..64]	**Key: <S: 0, 90>** Specifies the option key of your software option. These are added to the VCS in order to add extra functionality, such as increasing the VCS's capacity. Contact your TANDBERG representative for further information.		
Policy	**AdministratorPolicy**	**Mode: <On/Off>** Enables and disables use of Administrator Policy. On: Administrator Policy is in use. Off: Administrator Policy is not in use.	
	UserPolicy	**Mode: <Off/Local/Remote>** Determines the User Policy Manager usage and location. Off: User Policy Manager is not used. Local: the on-box User Policy Manager is used. Remote: the off-box User Policy Manager is used.	
		Server	**Address: <S: 0, 128>** Specifies the IP address or FQDN of the remote User Policy Manager.
			Password: <S: 0, 30> Specifies the password used by the VCS to log in and query the remote User Policy Manager
			Path: <S: 0, 255> Specifies the URL of the remote User Policy Manager.
			Protocol: <HTTP/HTTPS> Specifies the protocol used to connect to the remote User Policy Manager. HTTP: HTTP will be used. HTTPS: HTTPS will be used.
			UserName: <S: 0, 30> Specifies the user name used by the VCS to log in and query the remote User Policy Manager.

Registration	**AllowList [1..2500]**	**Pattern**	**String: <S: 0, 60>** Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.
			Type: <Exact/Prefix/Suffix/Regex> Determines the way in which the entry in the Allow List must match the alias. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression.
	DenyList [1..2500]	**Pattern**	**String: <S: 0, 60>** Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.
			Type: <Exact/Prefix/Suffix/Regex> Determines the way in which the entry in the Deny List must match the alias. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression
	RestrictionPolicy: <None/AllowList/DenyList> Specifies the policy to be used when determining which endpoints may register with the system. None: Allow Lists and Deny Lists will not be used. AllowList: the endpoint's alias must match an entry on the Allow List in order for it to be permitted to register. DenyList: the endpoint will not be permitted to register if its alias matches an entry on the Deny List.		
SIP	**Domains**	**Domain [1..20]**	**Name: <S: 0, 128>** Specifies a domain for which this VCS is authoritative.
	Mode: <On/Off> Determines whether or not the VCS will provide SIP registrar and SIP proxy functionality. On: the VCS will act as a SIP registrar/proxy. Off: the VCS will not act as a SIP registrar/proxy.		
	Registrar	**Mode: <On/Off>** Determines whether the box will act as a SIP registrar. On: the VCS will act as a DIP registrar. Off: the VCS will not act as a SIP registrar.	

Command Reference - xConfiguration

SIP cont...	Registration	ExpireDelta: <5..7200> Specifies the period within which a SIP endpoint must re-register with the VCS to prevent its registration expiring.	
		Proxy	**Mode: <Off/ProxyToKnownOnly/ProxyToAny>** Specifies how proxied registrations should be handled. Off: registration requests will not be proxied. ProxyToKnownOnly: registration requests will be proxied to neighbors only. ProxyToAny: Registration requests will be proxied in accordance with the VCS's existing call processing rules.
	TCP	**Mode: <On/Off>** Determines whether incoming SIP calls using the TCP protocol will be allowed. On: SIP calls using the TCP protocol will be allowed. Off: SIP calls using the TCP protocol will not be allowed	
		Port: <1024..65534> Specifies the listening port for incoming SIP TCP calls.	
	TLS	**Mode: <On/Off>** Determines whether incoming SIP calls using the TLS protocol will be allowed. On: SIP calls using the TLS protocol will be allowed Off: SIP calls using the TLS protocol will not be allowed	
		Port: <1024..65534> Specifies the listening port for incoming SIP TLS calls.	
	UDP	**Mode: <On/Off>** Determines whether incoming SIP calls using the UDP protocol will be allowed. On: SIP calls using the UDP protocol will be allowed. Off: SIP calls using the UDP protocol will not be allowed.	
		Port: <1024..65534> Specifies the listening port for incoming SIP UDP calls.	

Command Reference - xConfiguration

SNMP		**CommunityName: <S: 0, 16>** Sets the VCS's SNMP community name.
		Mode: <On/Off> Enables or disables SNMP support. On: SNMP support is enabled. Off: SNMP support is not enabled. Note: You must restart the system for any changes to take effect.
		SystemContact: <S: 0, 70> Specifies the name of the person who can be contacted regarding issues with the VCS.
		SystemLocation: <S: 0, 70> Specifies the physical location of the VCS.
SystemUnit		**Name: <S: 0, 50>** Defines the name of the VCS. Choose a name that uniquely identifies the system.
		Password: <S: 0, 16> Defines the password of the VCS. The password is used to login with Telnet, HTTP(S), SSH, SCP, and on the serial port.
TimeZone		**Name: <S: 0, 64>** Sets the local time zone of the VCS. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_York.
Transform [1..100]	**Pattern**	**String: <S: 0, 60>** Specifies the pattern against which the alias is compared.
		Type: <Exact/Prefix/Suffix/Regex> Determines the way in which the string must match the alias. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression.
		Behavior: <Strip/Replace> Determines how the matched part of the alias will be modified. Strip: the matching prefix or suffix will removed from the alias. Replace: the matching part of the alias will be substituted with the text in the Replace string.

Command Reference - xConfiguration

Transform [1..100] cont...	**Pattern cont...**	**Replace: <S: 0, 60>** (Applies only if pattern behavior is set to Replace.) Specifies the string to be used as a substitution for the part of the alias that matched the pattern.			
	Priority: <1..65534> Assigns a priority to the specified transform. Transforms are applied in order of priority, and the priority must be unique for each transform.				
Traversal	**Media**	**Port**	**Start: <1024..65534>** For traversal calls (i.e. where the VCS is taking the media as well as the signaling), specifies the lower port in the range to be used for the media.		
			End: <1024..65534> For traversal calls (i.e. where the VCS is taking the media as well as the signaling), specifies the upper port in the range to be used for the media.		
	Server	**H323**	**Assent**	**CallSignaling**	**Port: <1024..65534>** Specifies the port on the VCS to be used for Assent signaling.
			H46018	**CallSignaling**	**Port: <1024..65534>** Specifies the port on the VCS to be used for H.460.18 signaling.
		Media	**Demultiplexing**	**RTCP**	**Port: <1024..65534>** Specifies the port on the VCS to be used for demultiplexing RTCP media. Note: You must restart the system for any changes to take effect.
				RTP	**Port: <1024..65534>** Specifies the port on the VCS to be used for demultiplexing RTP media. Note: You must restart the system for any changes to take effect.
		STUN	**Discovery**	**Mode: <On/Off>** Determines whether the VCS will offer STUN discovery services to traversal clients. On: STUN discovery services are available. Off: STUN discovery services are not available.	
				Port: <1024..65534> Specifies the port to be used for STUN discovery services.	

Command Reference - xConfiguration

Traversal cont...	**Server cont..**	**STUN cont...**	**Relay**	**Mode: <On/Off>** Determines whether the VCS will offer STUN relay services to traversal clients. On: STUN relay services are available. Off: STUN relay services are not available.		
	.			**Port: <1024..65534>** Specifies the listening port for STUN relay requests.		
				Media	**Port**	**Start: <1024..65534>** Specifies the lower port in the range to be used for STUN media relay.
						End: <1024..65534> Specifies the upper port in the range to be used for STUN media relay.
Zones	**LocalZone**	**DefaultSubZone**	**Bandwidth**	**PerCall**	**Inter**	**Mode: <None/Limited/Unlimited>** Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in the Default Subzone. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
						Limit: <1..100000000> (applies only if Mode is set to Limited) Specifies the bandwidth limit (in kbps) for any one call to or from an endpoint in the Default Subzone.
					Intra	**Mode: <None/Limited/Unlimited>** Determines whether there is a limit on the bandwidth for any one call between two endpoints within the Default Subzone. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
						Limit: <1..100000000> (applies only if Mode is set to Limited) Specifies the bandwidth limit (in kbps) for any one call between two endpoints within the Default Subzone.

Command Reference - xConfiguration

Zones cont...	LocalZone cont...	DefaultSubZone cont...	Bandwidth cont...	Total		**Mode: <None/Limited/Unlimited>** Determines whether the Default Subzone has a limit on the total bandwidth being used by its endpoints at any one time. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
						Limit: <1..100000000> (applies only if Mode is set to Limited) Sets the total bandwidth limit (in kbps) of the Default Subzone.
		SubZone [1..100]	Bandwidth	PerCall	Inter	**Mode: <None/Limited/Unlimited>** Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
						Limit: <1..100000000> (applies only if Mode is set to Limited) Specifies the bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone
					Intra	**Mode: <None/Limited/Unlimited>** Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
						Limit: <1..100000000> (applies only if Mode is set to Limited) Specifies the bandwidth limit (in kbps) for any one call between two endpoints within this subzone.

Zones cont...	LocalZone cont...	SubZone [1..100] cont...	Bandwidth cont....	Total			**Mode: <None/Limited/Unlimited>** Determines whether this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
							Limit: <1..100000000> (applies only if Mode is set to Limited) Sets the total bandwidth limit (in kbps) of this subzone.
			Name: <S: 1, 50> Assigns a name to this subzone.				
			Subnet [1..5]	IP			**Address: <S: 0, 39>** Specifies an IP address used (in conjunction with the IP Prefix Length) to identify a subnet to be assigned to this subzone.
							PrefixLength: <0..128> Specifies the number of bits of the Subnet IP address which must match for an IP address to belong in this subzone.
		Traversal	H323	Assent			**Mode: <On/Off>** Determines whether or not H.323 calls using Assent mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the VCS. On: calls using Assent mode will be allowed. Off: calls using Assent mode will not be allowed.
				H46018			**Mode: <On/Off>** Determines whether or not H.323 calls using H.460.18 mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the VCS. On: calls using H.460.18 mode will be allowed. Off: calls using H.460.18 mode will not be allowed.
				H46019	Demultiplexing		**Mode: <On/Off>** Determines whether the VCS will operate in Demultiplexing mode for calls from traversal-enabled endpoints registered directly with it. On: allows use of the same two ports for all calls. Off: Each call will use a separate pair of ports for media.

Zones cont...	LocalZone cont...	Traversal cont...	H323 cont...	**Preference: <Assent/H46018>** If an endpoint that is registered directly with the VCS supports both Assent and H.460.18 protocols, this setting determines which the VCS uses. Assent: the Assent protocol will be used. H46018: the H.460.18 protocol will be used.	
				TCPProbe	**KeepAliveInterval: <1..65534>** Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
					RetryCount: <1..65534> Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a TCP probe to the VCS.
					RetryInterval: <1..65534> Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a TCP probe to the VCS.
				UDPProbe	**KeepAliveInterval: <1..65534>** Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
					RetryCount: <1..65534> Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a UDP probe to the VCS.
					RetryInterval: <1..65534> Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a UDP probe to the VCS.

Zones cont...	**LocalZone cont...**	**TraversalSubZone**	**Bandwidth**	**PerCall**	**Mode: <None/Limited/Unlimited>** Determines whether there is a limit on the bandwidth of any one traversal call being handled by the VCS. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
					Limit: <1..100000000> (applies only if Mode is set to Limited) Specifies the bandwidth limit (in kbps) applied to any one traversal call being handled by the VCS.
				Total	**Mode: <None/Limited/Unlimited>** Determines whether or not there is a limit to the total bandwidth of all traversal calls being handled by the VCS. None: no bandwidth will be available. Limited: there will be a limit on the bandwidth. Unlimited: there will be no limit on the bandwidth.
					Limit: <1..100000000> (applies only if Mode is set to Limited) Specifies the total bandwidth (in kbps) allowed for all traversal calls being handled by the VCS.
	Zone [1..200]	**ENUM**	**DNSSuffix: <S: 0, 128>** Specifies the domain to be appended to the transformed E.164 number to create an ENUM host name which this zone is then queried for.		
		H323	**Mode: <On/Off>** Determines whether H.323 calls will be allowed to and from this zone. On: H.323 calls will be allowed. Off: H.323 calls will not be allowed.		
		HopCount: <1..255> Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.			

Zones cont...	**Zone [1..200] cont...**	**Match [1..5]**		**Mode: <AlwaysMatch/PatternMatch/Disabled>** Determines if and when a query will be sent to this zone. Always: the zone will always be queried. Pattern: the zone will only be queried if the alias queried for matches the corresponding pattern. Disabled: the zone will never be queried.
			Pattern	**String: <S: 0, 60>** (applies only if the Match mode is Pattern Match) Specifies the pattern against which the alias is compared.
				Type: <Exact/Prefix/Suffix/Regex> (applies only if the Match mode is Pattern Match) Determines the way in which the string must match the alias. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression.
				Behavior: <Strip/Leave/Replace> (applies only if the Match mode is Pattern Match) Determines whether the matched part of the alias should be modified before an LRQ is sent to this zone. Leave: the alias will be unmodified. Strip: the matching prefix or suffix will be removed from the alias. Replace: the matching part of the alias will be substituted with the text in the Replace string.
				Replace: <S: 0, 60> (applies only if the Pattern Behavior is Replace) Specifies the string to be used as a substitution for the part of the alias that matched the pattern.
				Priority: <1..65534> Determines the order in which the zone will be sent a search request. Zones with priority 1 matches are searched first, followed by priority 2, and so on.
		Name: <S: 1, 50> Assigns a name to this zone.		

Zones cont...	Zone [1..200] cont...	Neighbor	Alternate [1..5]	**Address: <S: 0, 128>** Specifies the IP addresses or FQDNs of any Alternates configured on this neighbor.
			H323	**Port: <1024..65534>** Specifies the port on the neighbor to be used for H.323 calls to and from this VCS.
			Primary	**Address: <S: 0, 128>** Specifies the IP address or FQDN of this neighbor.
			SIP	**Port: <1024..65534>** Specifies the port on the neighbor to be used for SIP calls to and from this VCS.
				Transport: <TCP/TLS> Determines which transport type will be used for SIP calls to and from this neighbor. TCP: TCP will be used. TLS: TLS will be used.
		SIP	**Mode: <On/Off>** Determines whether SIP calls will be allowed to and from this zone. On: SIP calls will be allowed. Off: SIP calls will not be allowed.	
		TraversalClient	Alternate [1..5]	**Address: <S: 0, 128>** Specifies the IP address or FQDN of any Alternates of the traversal server.
			H323	**Port: <1024..65534>** Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this VCS.
				Protocol: <Assent/H46018> Determines which of the two firewall traversal protocols to use for calls to the traversal server when both are available. Assent: the Assent protocol will be used. H46018: the H.460.18 protocol will be used.
			Primary Address: <S: 0, 128> Specifies the IP address or FQDN of the traversal server.	
			RetryInterval: <1..65534> Specifies the interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried.	

Zones cont...	Zone [1..200] cont...	TraversalClient cont...	SIP	**Port: <1024..65534>** Specifies the port on the traversal server to be used for SIP calls from this VCS.		
				Transport: <TCP/TLS> Determines which transport type will be used for SIP calls to and from the traversal server. TCP: TCP will be used. TLS: TLS will be used.		
		TraversalServer	Authentication	**UserName: <S: 1, 128>** If the traversal client is a VCS, this must be the VCS's Authentication User Name. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name.		
			H323	H46019	Demultiplexing	**Mode: <On/Off>** Determines whether the VCS will operate in Demultiplexing mode for calls from the traversal client. On: allows use of the same two ports for all calls. Off: Each call will use a separate pair of ports for media.
				Port: <1024..65534> Specifies the port on the VCS being used for H.323 firewall traversal from this traversal client.		
				Protocol: <Assent/H46018> Determines the protocol to be used for calls from the traversal client. Assent: the Assent protocol will be used. H46018: the H.460.18 protocol will be used.		
			SIP	**Port: <1024..65534>** Specifies the port on the VCS being used for SIP firewall traversal from this traversal client.		
				Transport: <TCP/TLS> Determines which of the two transport types will be used for SIP calls between the traversal client and VCS. TCP: TCP will be used. TLS: TLS will be used.		

Command Reference - xConfiguration

Zones cont...	**Zone [1..200] cont...**	**TraversalServer cont...**	**TCPProbe**	**KeepAliveInterval: <1..65534>** Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
				RetryCount: <1..65534> Sets the number of times the traversal client will attempt to send a TCP probe to the VCS.
				RetryInterval: <1..65534> Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the VCS.
			UDPProbe	**KeepAliveInterval: <1..65534>** Sets the interval (in seconds) with which the traversal client will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
				RetryCount: <1..65534> Sets the number of times the traversal client will attempt to send a UDP probe to the VCS.
				RetryInterval: <1..65534> Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the VCS.
		Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS> Determines the nature of the specified zone, in relation to the Local Zone. Neighbor: the new zone will be a neighbor of the Local Zone. TraversalClient: there is a firewall between the zones, and the Local Zone is a traversal client of the new zone. TraversalServer: there is a firewall between the zones and the Local Zone is a traversal server for the new zone. ENUM: the new zone contains endpoints discoverable by ENUM lookup. DNS: the new zone contains endpoints discoverable by DNS lookup.		

Command Reference - xCommand

xCommand	Description	Parameters
AllowListAdd	Adds an entry to the Allow List.	**PatternString(r): <S: 1, 60>** Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted. **PatternType: <Exact/Prefix/Suffix/Regex>** Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly.
AllowListDelete	Deletes an entry from the Allow List.	**AllowListId(r): <1..2500>** The index of the entry to be deleted.
Boot	Reboots the VCS.	none
CheckBandwidth	A diagnostic tool that returns the status and route (as a list of nodes and links) that a call of the specified type and bandwidth would take between two nodes. Note that this command does not change any existing system configuration.	**Node1(r): <S: 1, 50>** The subzone or zone from which the call originates. **Node2(r): <S: 1, 50>** The subzone or zone at which the call terminates. **Bandwidth(r): <1..100000000>** The requested bandwidth of the call (in kbps). **CallType(r): <Traversal/NonTraversal>** Whether the call type is Traversal or Non Traversal.
CheckPattern	A diagnostic tool that allows you to check the result of an alias transform (local or zone) before you configure it on the system. Note that this command does not change any existing system configuration.	**Target(r): <S: 1, 60>** The original alias. **Pattern(r): <S: 1, 60>** The pattern against which the alias is to be compared. **Type(r): <Exact/Prefix/Suffix/Regex>** The way in which the pattern must match the alias in order for the transform to be applied. **Behavior(r): <Strip/Replace>** The way in which the alias will be modified. **Replace: <S: 1, 60>** (Applies only if Behavior is set to Replace.) The string to be substituted for the part of the alias that matched the pattern.

Command Reference - xCommand

xCommand	Description	Parameters
CredentialAdd	Adds an entry to the local authentication database.	**CredentialName(r): <S: 1, 128>** Defines the name for this entry in the local authentication database. **CredentialPassword(r): <S: 1, 128>** Defines the password for this entry in the local authentication database.
CredentialDelete	Deletes an entry from the local authentication database.	**CredentialId(r): <1..2500>** The index of the credential to be deleted.
DefaultLinksAdd	Restores links between the Default Subzone, Traversal Sub-zone and the Default Zone.	none
DefaultValuesSet	Resets system parameters to default values.	**Level(r): <1..3>** The level of system parameters to be reset. 1: Resets most parameters. 2: There are currently no level 2 parameters, so setting that level has the same effect as setting level 1. 3: Resets all level 1 and 2 parameters as well as additional parameters.
DenyListAdd	Adds an entry to the Deny List.	**PatternString(r): <S: 1, 60>** Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted. **PatternType: <Exact/Prefix/Suffix/Regex>** Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly.
DenyListDelete	Deletes an entry from the Deny List.	**DenyListId(r): <1..2500>** The index of the entry to be deleted.
DisconnectCall	Disconnects a call.	**Call: <1..900>** The index of the call to be disconnected. **CallSerialNumber: <S: 1, 255>** The serial number of the call to be disconnected.
DomainAdd	Adds a SIP domain for which this VCS is authoritative.	**DomainName(r): <S: 1, 128>** Specifies the name of the domain.
DomainDelete	Deletes a domain.	**DomainId(r): <1..20>** The index of the domain to be deleted.

xCommand	Description	Parameters
FeedbackDeregister	Deactivates a particular feedback request.	**ID: <1..3>** The ID of the feedback request to be deactivated.
FeedbackRegister	Activates notifications on the event or status change(s) described by the Expression(s). Notifications are sent in XML format to the specified URL. Up to 15 Expressions may be registered for each of 3 feedback IDs.	**ID: <1..3>** The ID of this particular feedback request. **URL(r): <S: 1, 256>** The URL to which notifications are to be sent. **Expression.1..15: <S: 1, 256>** The events or status change to be notified. Valid Expressions are: Status/Ethernet Status/NTP Status/LDAP Status/Feedback Status/ExternalManager Status/Calls Status/Registrations Status/Zones Event/CallAttempt Event/CallConnected Event/CallDisconnected Event/CallFailure Event/RegistrationAdded Event/RegistrationRemoved Event/RegistrationFailure Event/RegistrationChanged Event/Bandwidth Event/Locate Event/ResourceUsage Event/AuthenticationFailure
FindRegistration	Returns information about the registration associated with the specified alias. The alias must be registered on the VCS on which the command is issued.	Alias(r): <S: 1, 60> The alias that you wish to find out about.

Command Reference - xCommand

xCommand	Description	Parameters
LinkAdd	Adds and configures a new link.	**LinkName(r): <S: 1, 50>** Assigns a name to this link. **Node1: <S: 1, 50>** Specifies the first zone or subzone to which this link will be applied. **Node2: <S: 1, 50>** Specifies the second zone or subzone to which this link will be applied. **Pipe1: <S: 1, 50>** Specifies the first pipe to be associated with this link. **Pipe2: <S: 1, 50>** Specifies the second pipe to be associated with this link.
LinkDelete	Deletes a link.	**LinkId(r): <1..600>** The index of the link to be deleted.
Locate	Runs the VCS's location algorithm to locate the endpoint identified by the given alias, searching locally, on neighbors, and on systems discovered through the DNS system, within the specified number of "hops". Results are reported back through the xFeedback mechanism, which must therefore be activated before issuing this command (e.g. xFeedback register event/locate).	**Alias(r): <S: 1, 60>** The alias associated with the endpoint you wish to locate. **HopCount(r): <0..255>** The hop count to be used in the search. **Protocol(r): <H323/SIP>** The protocol used to initiate the search.
OptionKeyAdd	Adds a new option key to the VCS.	**Key(r): <S: 0, 90>** Specifies the key of the software option to be added.
OptionKeyDelete	Deletes a software option key from the VCS.	**OptionKeyId(r): <1..64>** Specifies the ID of the software option to be deleted.

Command Reference - xCommand

xCommand	Description	Parameters
PipeAdd	Adds and configures a new pipe.	**PipeName(r): <S: 1, 50>** Assigns a name to this pipe. **TotalMode: <None/Limited/Unlimited>** Determines whether or not this pipe is enforcing total bandwidth restrictions. None: no bandwidth available. **Total: <1..100000000>** If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. **PerCallMode: <None/Limited/Unlimited>** Determines whether or not this pipe is limiting the bandwidth of individual calls. None: no bandwidth available. **PerCall: <1..100000000>** If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call.
PipeDelete	Deletes a pipe.	**PipeId(r): <1..100>** The index of the pipe to be deleted.
RemoveRegistration	Removes a registration from the VCS.	**Registration: <1..3750>** The index number of the registration to be removed. **RegistrationSerialNumber: <S: 1, 255>** The serial number of the registration to be removed.

xCommand	Description	Parameters
SubZoneAdd	Adds and configures a new subzone.	**SubZoneName(r): <S: 1, 50>** Assigns a name to this subzone. **Address: <S: 0, 39>** Specifies an IP address used (in conjunction with the IP Prefix Length) to identify a subnet to be assigned to this subzone. **PrefixLength: <0..128>** Specifies the number of bits of the Subnet IP address which must match for an IP address to belong in this subzone. **TotalMode: <None/Limited/Unlimited>** Determines whether this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time. **Total: <1..100000000>** Sets the total bandwidth limit (in kbps) of this subzone (applies only if Mode is set to Limited). **PerCallInterMode: <None/Limited/Unlimited>** Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone. **PerCallInter: <1..100000000>** Specifies the bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if Mode is set to Limited). **PerCallIntraMode: <None/Limited/Unlimited>** Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone. **PerCallIntra: <1..100000000>** Specifies the bandwidth limit (in kbps) on any one call between two endpoints within this subzone.
SubZoneDelete	Deletes a subzone.	**SubZoneId(r): <1..100>** The index of the subzone to be deleted.

xCommand	Description	Parameters
TransformAdd	Adds and configures a new transform.	**Pattern(r): <S: 1, 60>** Specifies the pattern against which the alias is compared. **Type: <Exact/Prefix/Suffix/Regex>** Determines the way in which the string must match the alias. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression. **Behavior: <Strip/Replace>** Determines how the matched part of the alias will be modified. Strip: the matching prefix or suffix will removed from the alias. Replace: the matching part of the alias will be substituted with the text in the Replace string. **Replace: <S: 1, 60>** (Applies only if pattern behavior is set to Replace.) Specifies the string to be used as a substitution for the part of the alias that matched the pattern. **Priority: <1..65534>** Assigns a priority to the specified transform. Transforms are applied in order of priority, and the priority must be unique for each transform.
TransformDelete	Deletes a transform.	**TransformId(r): <1..100>** The index of the transform to be deleted.
ZoneAdd	Adds and configures a new zone.	**ZoneName(r): <S: 1, 50>** Assigns a name to this zone. **Type(r): <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>** Determines the nature of the specified zone, in relation to the Local Zone. Neighbor: the new zone will be a neighbor of the Local Zone. TraversalClient: there is a firewall between the zones, and the Local Zone is a traversal client of the new zone. TraversalServer: there is a firewall between the zones and the Local Zone is a traversal server for the new zone. ENUM: the new zone contains endpoints discoverable by ENUM lookup. DNS: the new zone contains endpoints discoverable by DNS lookup.
ZoneDelete	Deletes a zone.	**ZoneId(r): <1..200>** The index of the zone to be deleted.

xCommand	Description	Parameters
ZoneList	A diagnostic tool that returns the list of zones (grouped by priority) that would be queried, and any transforms that would be applied, in a search for a given alias. Note that this command does not change any existing system configuration.	**Alias(r): <S: 1, 60>** The alias to be searched for.

Command Reference - xStatus

SystemUnit:

- Product: “the product name”
- Uptime: <Time in seconds>
- SystemTime: <Time not set/date-time>
- TimeZone: <GMT or one of 300 other timezones>
- LocalTime: <local-date-time>
- Software:
    - Version: “the version number”
    - Build: <Number/Uncontrolled>
    - Name: “Release”
    - ReleaseDate: <Date>
    - Configuration:
        - NonTraversalCalls: <0..500>
        - TraversalCalls: <0..100>
        - Registrations: <0..2500>
        - BorderController: <True/False>
        - Encryption: <True/False>
        - Interworking: <True/False>
        - UserPolicy: <True/False>
    - Hardware:
        - Version: “1.0”
        - SerialNumber:

Ethernet:

- MacAddress: <S: 17>
- Speed: <10half/10full/100half/100full/1000full/down>

Options:

- Option [1-64]:
- Key: <S: 1, 90>
- Description: <S: 1, 128>

IP:

Protocol: <IPv4/IPv6/Both>

IPv4:

Address: <IPv4Addr>

SubnetMask: <IPv4Addr>

Gateway: <IPv4Addr>

IPv6:

Address: <IPv6Addr>

Gateway: <IPv6Addr>

DNS:

Server [1-5]:

Address: <IPv4Addr/IPv6Addr>

Domain: <S: 0, 128>

NTP:

Status: <Inactive/Active/Failed>

Cause: {Visible if status is Failed} <No response from NTP server/ DNS resolution failed

Address: <IPv4Addr/IPv6Addr>

Port: <1..65534>

Last Update: <date-time>

Last Correction: <Time in seconds, precision in seconds>

LDAP:

Status: <Inactive/Initializing/Active/Failed>

Cause: {Visible if status is Failed} <Failed to connect to LDAP server/ Failed to negotiate TLS with LDAP server/ Failed to perform TLS handshake with LDAP server/ Failed to authenticate with LDAP server/ DNS resolution failed>

Address: <IPv4Addr/IPv6Addr>

Port: <1..65534>

Command Reference - xStatus

External Manager:

- Status: <Inactive/Initializing/Active/Failed>
- Cause: {Visible if status is Failed} <DNS resolution failed >
- Address: <IPv4Addr/IPv6Addr >
- Protocol: HTTP
- URL: <S: 0, 255>

Feedback [1..3]:

- Status: <On/Off>
- URL: <S: 1,255>
- Expression: <S: 1,127> {0..15 entries}

ResourceUsage:

- Calls:
  - Traversal:
    - Current: <0..150>
    - Maximum: <0..150>
    - Total: <0..4294967295>
  - NonTraversal:
    - Current: <0..750>
    - Maximum: <0..750>
    - Total: <0..4294967295>
- Registrations:
  - Current: <0..3750>
  - Maximum: <0..3750>
  - Total: <0..4294967295>

- **Calls:**
  - Call <1..900>:
    - SerialNumber: <S: 1,255>
    - State: <Connecting/Connected/Disconnecting>
    - StartTime: <Seconds since boot/Date Time>
    - Duration: <Time in seconds, precision in seconds>
    - Legs:
      - Leg [1..300]:
        - Protocol: <H323/SIP>
        - H323: {visible if Protocol = H323}
          - CallSignalAddress: <IPv4Addr/[IPv6Addr]>:<1..65534>
          - Aliases:
            - Alias [1..50]:
              - Type: <E164/H323Id>
              - Value: <S: 1,60>
        - SIP: {visible if Protocol = SIP}
          - Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
          - Transport: <UDP/TCP/TLS/undefined>
          - Aliases:
            - Alias [1..50]:
              - Type: <URL>
              - Value: <S: 1,60>
        - Targets:
          - Target [1..1]:
            - Type: <E164/H323Id/URL>
            - Value: <S: 1,60>
        - BandwidthNode: <S: 1,50 Node name>
          - Registration:
            - ID: <1..2500>
            - SerialNumber: <S: 1,255>
    - Sessions:
      - Session: [1..300:]
        - Status: <Unknown/Searching/Failed/Cancelled/Completed/Active/Connected>

Calls *continued...*

- MediaRouted: <True/False>
- Participants:
  - Leg: <1..300> {2 entries}
- Bandwidth: <0..100000000> kbps
- Route:
  - Zone/Link: <S: 1,50 Node name> {0..150 entries}

Registrations:

- Registration [1..3750]:
  - Protocol: <H323/SIP>
  - Node: <S: 1,50 Node name>
  - SerialNumber: <S: 1,255>
  - CreationTime: <Date Time>
  - SecondsSinceLastRefresh: <1..65534> {Visible if Protocol is SIP}
  - SecondsToExpiry <1..65534> {Visible if Protocol is SIP}
  - VendorInfo: <S: 1,255>
  - H323: {Visible if Protocol is H323}
    - Type: <Endpoint/MCU/Gateway/Gatekeeper>:
    - CallSignalAddresses:
      - Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
    - RASAddresses:
      - Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
      - Apparent: <IPv4Addr/[IPv6Addr]>:<1..65534>
    - Prefix: <S: 1,20> {0..50 entries}
    - Aliases:
      - Alias [1..50]:
        - Type: <E164/H323Id/URL/GW Prefix/MCU Prefix/Prefix/Suffix/IPAddress>
        - Origin: <Endpoint/LDAP/Combined>
        - Value: <S: 1,60>
    - Traversal: <Assent/H46018> {Visible for Traversal calls}
  - SIP: {Visible if Protocol is SIP}
    - AOR: <S: 1,128>

Registrations *continued...*

Contact: <S: 1,255>
Path:
URI [1..10]: <S: 1,255>

Zones:

DefaultZone:
Name: “DefaultZone”
Bandwidth:
Used: <0..100000000>
Calls:
Call [0..900]: {0..900 entries}
CallSerialNumber: <S: 1,255>
LocalZone:
DefaultSubZone:
Name: “DefaultSubZone”
Bandwidth:
Used: <0..100000000>
Registrations: {0..3750 entries}
Registration: <1..3750>
SerialNumber: <S: 1,255>
Calls:
Call [0..900]: {0..900 entries}
CallSerialNumber: <S: 1,255>
TraversalSubZone:
Name: “TraversalSubZone”
Bandwidth:
Used: <0..100000000>
Calls:
Call [0..900]: {0..900 entries}
CallSerialNumber: <S: 1,255>
SubZone: [1.100]
Name: <S: 1,50 Node name>

Zones *continued...*

- Bandwidth:
  - Used: <0..100000000>
- Registrations: {0..3750 entries}
  - Registration: <1..3750>
    - SerialNumber: <S: 1,255>
- Calls:
  - Call [0..900]: {0..900 entries}
  - CallSerialNumber: <S: 1,255>

Searches:

- Current:
- Total:
- Dropped:

Zone [1..200]:

- Name: <S: 1,50 Node name>
- Status: <Active/Failed/Warning>
- Cause: {Visible if status is Failed or Warning} <No gatekeeper reachable/ Gatekeepers unreachable>
- Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>
- Neighbor: {Visible if Type is Neighbor}
  - Primary:
    - H323: {Visible if H323 Mode=On for Zone}
      - Status: <Unknown/Active/Failed>
      - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
      - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
      - Port: <1..65534>
      - LastStatusChange: <Time not set/Date Time>
    - SIP: {Visible if SIP Mode=On for Zone}
      - Status: <Unknown/Active/Failed>
      - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
      - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
      - Port: <1..65534>
      - LastStatusChange: <Time not set/Date Time>
  - Alternate [1..5]:

Zones *continued...*

- H323: {Visible if H323 Mode=On for Zone}
  - Status: <Unknown/Active/Failed>
  - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
  - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
  - Port: <1..65534>
  - LastStatusChange: <Time not set/Date Time>
- SIP: {Visible if SIP Mode=On for Zone}
  - Status: <Unknown/Active/Failed>
  - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
  - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
  - Port: <1..65534>
  - LastStatusChange: <Time not set/Date Time>

TraversalClient: {Visible if Type is TraversalClient}

- Primary:
  - H323: {Visible if H323 Mode=On for Zone}
    - Status: <Unknown/Active/Failed>
    - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
    - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
    - Port: <1..65534>
    - LastStatusChange: <Time not set/Date Time>
  - SIP: {Visible if SIP Mode=On for Zone}
    - Status: <Unknown/Active/Failed>
    - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
    - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
    - Port: <1..65534>
    - LastStatusChange: <Time not set/Date Time>
- Alternate [1..5]:
  - H323: {Visible if H323 Mode=On for Zone}
    - Status: <Unknown/Active/Failed>
    - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
    - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
    - Port: <1..65534>

Command Reference - xStatus

Zones *continued...*

            - LastStatusChange: <Time not set/Date Time>
        - SIP: {Visible if SIP Mode=On for Zone}
            - Status: <Unknown/Active/Failed>
            - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
            - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
            - Port: <1..65534>
            - LastStatusChange: <Time not set/Date Time>
- TraversalServer: {Visible if Type is TraversalServer}
    - SIP:
        - Port: <Active/Inactive>
    - H323:
        - Port: <Active/Inactive>
    - Primary:
        - H323: {Visible if H323 Mode=On for Zone}
            - Status: <Unknown/Active/Failed>
            - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
            - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
            - Port: <1..65534>
            - LastStatusChange: <Time not set/Date Time>
        - SIP: {Visible if SIP Mode=On for Zone}
            - Status: <Unknown/Active/Failed>
            - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
            - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
            - Port: <1..65534>
            - LastStatusChange: <Time not set/Date Time>
    - Alternate [1..5]:
        - H323: {Visible if H323 Mode=On for Zone}
            - Status: <Unknown/Active/Failed>
            - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
            - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
            - Port: <1..65534>
            - LastStatusChange: <Time not set/Date Time>

Zones *continued...*

SIP: {Visible if SIP Mode=On for Zone}
    Status: <Unknown/Active/Failed>
    Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
    Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
    Port: <1..65534>
    LastStatusChange: <Time not set/Date Time>
Calls: {0..900 entries}
    Call [0..900]:
        CallSerialNumber: <S: 1,255>

Links:

Link [1..100]:
    Name: <S: 1,50 Link name>
    Bandwidth:
        Used: <0..100000000>
    Calls:
        Call [0..900]: {0..900 entries}
            CallSerialNumber: <S: 1,255>

Pipes:

Pipe [1..100]:
    Name: <S: 1,50 Pipe name>
    Bandwidth:
        Used: <0..100000000>
    Calls:
        Call [0..900]: {0..900 entries}
            CallSerialNumber: <S: 1,255>

Alternates:

- Alternate [1..5]:
  - Status: <Active/Failed/Unknown>
  - Cause: {Visible if status is Failed} <No response from gatekeeper/DNS resolution failed/Invalid IP address>
  - Address: <IPv4Addr/IPv6Addr>
  - Port: <1..65534>
  - LastStatusChange: <Seconds since boot/Date Time>

UserPolicyManager:

- Mode: <Off/Local/Remote>
- Status: <Active/Inactive/Unknown> {Visible if Remote}
- Address: <1..1024> {Visible if Remote}

H323:

- Registration:
  - Status: <Active/Inactive/Failed>
  - IPv4: {Visible if Status=Active}
    - Address: <IPv4Addr>
  - IPv6: {Visible if Status=Active}
    - Address: <IPv6Addr>
- CallSignaling:
  - Status: <Active/Inactive/Failed>
  - IPv4: {Visible if Status=Active}
    - Address: <IPv4Addr>
  - IPv6: {Visible if Status=Active}
    - Address: <IPv6Addr>
- Assent:
  - CallSignaling:
    - Status: <Active/Inactive/Failed>
    - IPv4: {Visible if Status=Active}
      - Address: <IPv4Addr>
    - IPv6: {Visible if Status=Active}
      - Address: <IPv6Addr>

H323 *continued...*

- H46018:
  - CallSignaling:
    - Status: <Active/Inactive/Failed>
    - IPv4: {Visible if Status=Active}
      - Address: <IPv4Addr>
    - IPv6: {Visible if Status=Active}
      - Address: <IPv6Addr>

SIP:

- IPv4:
  - UDP:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv4Addr>
  - TCP:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv4Addr>
  - TLS:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv4Addr>
- IPv6:
  - UDP:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv6Addr>
  - TCP:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv6Addr>
  - TLS:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv6Addr>

STUN:

- Servers:
  - Discovery:
    - Status: <Active/Inactive>
    - Address: <IPv4Addr/IPv6Addr>
  - Relay:
    - Status: <Active/Inactive>
    - Address: <IPv4Addr/IPv6Addr>
    - Bindings:
      - Count: <0..800>
      - Binding [1..800]:
        - Client: <IPv4Addr/IPv6Addr>
        - CreationTime: <Date Time>
        - ExpireTime: <Date Time>

Warnings:

- Warning [1..n]:
  - Value: <S: 1,255>

Overview

This Appendix gives details of the VCS's implementation of the CPL language and should be read in conjunction with the CPL standard RFC 3880 (5).

The VCS supports most of the CPL standard along with some TANDBERG-defined extensions. It does not support the top level actions `<incoming>` and `<outgoing>` as described in RFC 3880. Instead it supports a single section of CPL within a `<routed>` section.

When Administrator Policy is implemented by uploading a CPL script to the VCS, the script is checked against an XML schema to verify the syntax. There are two schemas - one for the basic CPL specification and one for the TANDBERG extensions. Both these schemas can be viewed from the web interface. and used to validate your script before uploading to the VCS.

The following example shows the correct use of namespaces to make the syntax acceptable:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="destination">
    <address is="reception@example.com">
       <proxy/>
    </address>
  </address-switch>
</taa:routed>
</cpl>
```

address-switch node

The address-switch node allows the script to run different actions based on the source or destination aliases of the call. It specifies which fields to match and then a list of address nodes contains the possible matches and their associated actions.

The address-switch has two node parameters: Field and Subfield.

address

The address construct is used within an address-switch to specify addresses to match. It supports the use of Regular Expressions (see Regular Expression Reference for further information).

`is=`*string*	Selected field and subfield exactly match the given *string*.
`contains=`*string*	Selected field and subfield contain the given *string*. Note: The CPL standard only allows for this matching on the display subfield; however the VCS allows it on any type of field.
`subdomain-of=`*string*	If the selected field is numeric (e.g. the `tel` subfield) then this matches as a prefix; so `address subdomain-of="555"` matches `5556734` etc. If the field is not numeric then normal domain name matching is applied; so `address subdomain-of="company.com"` matches `nodeA.company.com` etc.
regex="regular expression"	Selected field and subfield match the given regular expression.

All address comparisons ignore upper/lower case differences so `address is="Fred"` will also match `fred`, `freD` etc.

otherwise node

The `otherwise` node will be executed if the address specified in the address-switch was found but none of the preceding address nodes matched.

not-present node

The `not-present` node is executed when the address specified in the address-switch was not present in the call setup message. This form is most useful when authentication is being used. With authentication enabled the VCS will only use authenticated aliases when running policy so the `not-present` action can be used to take appropriate action when a call is received from an unauthenticated user (see the example call screening of unauthenticated users).

Overview

Field

Within the address-switch node, the mandatory field parameter specifies which address is to be considered. The supported attributes and their interpretation are as follows:

	Authentication Mode: On		Authentication Mode: Off	
Field	SIP	H.323	SIP	H.323
origin	The “From” and “ReplyTo” fields of the message if it authenticated correctly, otherwise not-present.	The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly otherwise not-present. Since SETUP messages are not authenticated if we receive a setup without a preceding RAS message the origin will always be not-present.	The “From” and “ReplyTo” fields of the incoming message.	The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.
unauthenticated-origin	The “From” and “ReplyTo” fields of the incoming message.	The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.	The “From” and “ReplyTo” fields of the incoming message.	The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.
authenticated-origin	The “From” and “ReplyTo” fields of the message if it authenticated correctly, otherwise not-present.	The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly otherwise empty. Since SETUP messages are not authenticated if we receive a setup without a preceding RAS message the origin will always be not-present.	not-present	
originating-zone	The name of the zone or subzone for the originating leg of the call. If the call originates from a Neighbor, Traversal Server or Traversal Client zone then this will equate to the zone name. If it comes from an endpoint within one of the local subzones this will be the name of the subzone. If the call originates from any other locally registered endpoint this will be “DefaultSubZone”. In all other cases this will be “DefaultZone”.			
originating-user	The username used for authentication.		not-present	
registered-origin	If the call originates from a registered endpoint this is the list of all aliases it has registered, otherwise not-present.			
destination	The destination aliases.			
original-destination	The destination aliases.			

If the selected field contains multiple aliases then the VCS will attempt to match each address node with all of the aliases before proceeding to the next address node i.e. an address node matches if it matches any alias.

Subfield

Within the address-switch node, the optional subfield parameter specifies which part of the address is to be considered. The following table gives the definition of subfields for each alias type.

If a subfield is not specified for the alias type being matched then the **not-present** action will be taken.

address-type	Either h323. or sip, based on the type of endpoint that originated the call.
user	For URI aliases this selects the username part. For H.323 IDs it is the entire ID and for E.164 numbers it is the entire number.
host	For URI aliases this selects the domain name part. If the alias is an IP address then this subfield is the complete address in dotted decimal form.
tel	For E.164 numbers this selects the entire string of digits.
alias-type	Gives a string representation of the type of alias. The type is inferred from the format of the alias. Possible types are: • Address Type • Result • URI • url-ID • H.323 ID • h323-ID • Dialled Digits • dialedDigits

Overview

CPL Script Actions

location

As the CPL script is evaluated it maintains a list of addresses (H.323 IDs, URLs and E.164 numbers) which will be used as the destination of the call if a proxy node is executed. The location node allows the location set to be modified so that calls can be redirected to different destinations.

At the start of script execution the location set is initialized to empty for incoming calls and to the original destination for outgoing calls.

The following attributes are supported on location nodes. It supports the use of Regular Expressions (see Regular Expression Reference for further information).

Clear = "yes" | "no"	Specifies whether to clear the current location set before adding the new location. The default is to append this location to the end of the set.
url=*string*	The new location to be added to the location set. The given string can specify a URL (e.g. user@domain.com), H.323 ID or an E.164 number.
priority=<0.0..1.0> | "random"	Specified either as a floating point number in the range 0.0 to 1.0, or random, which assigns a random number within the same range. 1.0 is the highest priority. Locations with the same priority are searched in parallel.
regex="<regular expression>" replace="<string>"	Specifies the way in which a location matching the regular expression is to be changed.

proxy

On executing a proxy node the VCS will attempt to forward the call to the locations specified in the current location set. If multiple entries are in the location set then this results in a forked call. If the current location set is empty the call will be forwarded to its original destination.

reject

If a reject node is executed the VCS stops any further script processing and rejects the current call. The custom reject strings status=*string* and reason=*string* options are supported here.

rule-switch

This extension to CPL is provided to simplify administrator policy scripts that need to make decisions based on both the source and destination of the call. A rule-switch may contain any number of rules that are tested in sequence; as soon as a match is found the CPL within that rule element is executed. Each rule must take one of the following forms:

```
<rule origin="<regular expression>" destination="<regular expression">

<rule authenticated-origin="<regular expression>" destination="<regular
expression">

<rule unauthenticated-origin="<regular expression>" destination="<regular
expression">

<rule registered-origin="<regular expression>" destination="<regular
expression">

<rule originating-user="<regular expression>" destination="<regular
expression">

<rule originating-zone="<regular expression>" destination="<regular
expression">
```

The meaning of the various origin selectors is as described in the Field parameter of address-switch.

Unsupported CPL Elements

The VCS does not currently support some elements that are described in the CPL RFC. If an attempt is made to upload a script containing any of the following elements an error message will be generated and the VCS will continue to use its existing policy.

The following elements are not currently supported:

- time-switch
- string-switch
- language-switch
- priority-switch
- redirect
- mail
- log
- subaction
- lookup
- remove-location

CPL Examples

Call Screening of Authenticated Users

In this example, only calls from users with authenticated source addresses are allowed.

See Authentication for details on how to enable authentication.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
        xmlns:taa="http://www.tandberg.net/cpl-extensions"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="origin">
    <not-present>
      <reject/>
    </not-present>
  </address-switch>
</taa:routed>
</cpl>
```

Call Screening Based on Alias

In this example, user ceo will only accept calls from users vpsales, vpmarketing or vpengineering.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
        xmlns:taa="http://www.tandberg.net/cpl-extensions"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="destination">
    <address is="ceo">
        <address-switch field="origin">
            <address regex="vpsales|vpmarketing|vpengineering">
                <proxy/>
            </address>
            <otherwise>
                <reject/>
            </otherwise>
            <not-present>
                <reject/>
            </not-present>
        </address-switch>
    </address>
  </address-switch>
</taa:routed>
</cpl>
```

CPL Examples

Call Screening Based on Domain

In this example, user fred will not accept calls from anyone at annoying.com, or from any unauthenticated users. All other users will allow any calls.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
        xmlns:taa="http://www.tandberg.net/cpl-extensions"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="destination">
      <address is="fred">
          <address-switch field="origin" subfield="host">
              <address subdomain-of="annoying.com">
                  <reject/>
              </address>
              <otherwise>
                  <proxy/>
              </otherwise>
              <not-present>
                  <reject/>
              </not-present>
          </address-switch>
      </address>
  </address-switch>
</taa:routed>
</cpl>
```

Change of Domain Name

In this example, Example Inc has changed its domain from example.net to example.com. For a period of time some users are still registered at example.net. The following script would attempt to connect calls to user@example.com first and if that fails then fallback to example.net.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="destination">
    <address regex="(.*)@example.com">
        <proxy>
            <failure>
              <location clear="yes" regex="(.*)@example.com" replace="\1@
example.net">
                 <proxy/>
              </location>
            </failure>
         </proxy>
    </address>
  </address-switch>
</taa:routed>
</cpl>
```

CPL Examples

Allow Calls from Locally Registered Endpoints Only

In this example, the administrator only wants to allow calls that originate from locally registered endpoints.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="registered-origin">
      <not-present>
          <reject reason="Only local endpoints can use this Tandberg VCS"/>
      </not-present>
  </address-switch>
</taa:routed>
</cpl>
```

Block Calls from Default Zone and Default Subzone

The same script can be extended to also allow calls from configured zones but not from the Default Zone or Default Subzone.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="registered-origin">
      <not-present>
          <address-switch field="originating-zone">
             <address is="DefaultZone">
               <reject/>
             </address>
             <address is="DefaultSubZone">
               <reject/>
             </address>
            <otherwise>
               <proxy/>
            </otherwise>
      </not-present>
  </address-switch>
</taa:routed>
</cpl>
```

CPL Examples

Restricting Access to a Local Gateway

In this example, a gateway is registered to the VCS with a prefix of 9 and the administrator wants to stop calls from outside the organization being routed through it.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="destination">
      <address regex="9(.*)">
        <address-switch field="originating-zone">
           <address is="TraversalZone1">
              <reject/>
           </address>
        </address-switch>
      </address>
  </address-switch>
</taa:routed>
</cpl>
```

Regular Expression Reference

About Regular Expressions

Regular expressions can be used in conjunction with a number of VCS features such as alias transformations, zone transformations, CPL policy and ENUM. The VCS uses POSIX format regular expression syntax.

This section provides a list of commonly used special characters in regular expression syntax.

For an example of regex usage, see CPL Examples.

For a detailed description of regular expression syntax see [9].

Character	Description	Example
.	Matches any character.	
*	Matches 0 or more repetitions of the previous match.	.* will match against any sequence of characters.
+	Matches 1 or more repetitions of the previous match.	
\	Escapes a regular expression special character.	
\d	Matches any decimal digit, i.e. 0-9.	
[...]	Matches a set of characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the - character and then the last character in the range. You can not use special characters within the [] - they will be taken literally.	[a-z] will match against any lower case alphabetical character. [a-zA-Z] will match against any alphabetical character. [0-9#*] will match against any single E.164 character - the E.164 character set is made up of the digits 0-9 plus the hash key (#) and the asterisk key (*).
(...)	Groups a set of matching characters together. Groups can then be referenced in order using the characters \1, \2, etc. as part of a replace string.	A regular expression can be constructed to transform a URI containing a user's full name to a URI based on their initials. The regular expression (.).* _ (.).*(@example.com) would match against the user john _ smith@example.com and with a replace string of \1\2\3 would transform it to js@example.com.
|	Matches against one expression or an alternate expression.	.*@example.(net|com) will match against any URI for the domain example.com or the domain example.net.
^	Signifies the start of a line.	
$	Signifies the end of a line.	^\d\d\d$ will match any string that is exactly 3 digits long.
(?!...)	Negative lookahead. Defines a subexpression that must not be present in order for there to be a match.	(?!.*@tandberg.net$).* will match any string that does not end with @tandberg.net.

DNS Configuration

Overview

This section gives examples of DNS configuration using Microsoft DNS Server and BIND 8 & 9.

In these examples we show how to set up an SRV record to handle H.323 URIs of the form user@example.com. These are handled by the system with the fully qualified domain name of vcs.example.com which is listening on port 1719, the default registration port.

It is assumed that both A and AAAA records already exist for vcs.example.com. If not, you will need to add one.

Verifying the SRV Record

There are a range of tools available to investigate DNS records. One commonly found on Microsoft Windows and UNIX platforms is `nslookup`. Use this to verify that everything is working as expected.

For example:

- `nslookup -querytype=srv _h323ls._udp.example.com`

and check the output.

Microsoft DNS Server

Using Microsoft DNS Server you can add the SRV record using either the command line or the MMC snap-in.

To use the command line, on the DNS server open a command window and enter:

- `dnscmd . /RecordAdd domain service_name SRV Priority Weight Port Target`

where:

`domain`	is the domain into which you wish to insert the record
`service_name`	is the name of the service you're adding
`Priority`	is the priority as defined by RFC 2782 [3]
`Weight`	is the weight as defined by RFC 2782 [3]
`Port`	is the port on which the system hosting the domain is listening
`Target`	is the FQDN of the system hosting the domain

For example:

- `dnscmd . /RecordAdd example.com _h323ls._udp SRV 1 0 1719 vcs.example.com`

BIND 8 & 9

BIND is a commonly used DNS server on UNIX and Linux systems. Configuration is based around two sets of text files: `named.conf` which describes which zones are represented by the server, and a selection of zone files which describe the detail of each zone.

BIND is sometimes run chrooted for increased security. This gives the program a new root directory, which means that the configuration files may not appear where you expect them to be. To see if this is the case on your system, run

- `ps aux grep named`

This will give the command line that named (the BIND server) was invoked with. If there is a `-t` option, then the path following that is the new root directory and your files will be located relative to that root.

In `/etc/named.conf` look for a directory entry within the options section. This will give the directory in which the zone files are stored, possibly relative to a new root directory. In the appropriate zone section, a file entry will give the name of the file containing the zone details.

For more details of how to configure BIND servers and the DNS system in general see [6].

LDAP Configuration

About the LDAP Databases

The VCS can be configured to use a database on an LDAP Directory Server to store authentication credential information (usernames, passwords, and other relevant information)

This section describes how to download the schemas that must be installed on the LDAP server, and how to install and configure two common types of LDAP servers, Microsoft Active Directory and OpenLDAP, for use with the VCS.

Downloading the H.350 schemas

The following ITU specification describes the schemas which are required to be installed on the LDAP server:

H.350	Directory services architecture for multimedia conferencing - An LDAP schema to represent endpoints on the network.
H.350.1	Directory services architecture for H.323 - An LDAP schema to represent H.323 endpoints.
H.350.2	Directory services architecture for H.235 - An LDAP schema to represent H.235 elements.

The schemas can be downloaded in `ldif` format from the web interface on the VCS. To do this:

1. Navigate to *VCS Configuration > Authentication > LDAP > Schemas*. You will see a list of downloadable schemas.
2. Click on the Download button next to each file to open it.

Microsoft Active Directory

Prerequisites

These step-by-step instructions assume that Active Directory has already been installed. For details on installing Active Directory please consult your Windows documentation.

The following instructions are for Windows Server 2003 Enterprise Edition. If you are not using this version of Windows, your instructions may vary.

Installing the H.350 Schemas

Once you have downloaded the H.350 schemas, install them as follows:

Open a command prompt and for each file execute the following command:

```
ldifde -i -c DC=X <ldap _ base> -f filename.ldf
```

where:

`<ldap _ base>` is the base DN for your Active Directory server.

Adding H.350 Objects

Create the Organizational Hierarchy

1. Open up the Active Directory Users and Computers MMC snap-in.
2. Under your BaseDN right-click and select New Organizational Unit.
3. Create an Organizational unit called h350.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the VCS read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 Objects

1. Create an ldif file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,DC=X
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
```

2. Add the ldif file to the server using the command:
   `ldifde -i -c DC=X <ldap _ base> -f filename.ldf`

   where:

   `<ldap _ base>` is the base DN of your Active Directory Server.

The example above will add a single H.323 endpoint with an H.323 Id alias of MeetingRoom1 and an E.164 alias of 626262. The entry also has H.235 credentials of id meetingroom1 and password mypassword which are used during authentication.

Securing with TLS

To enable Active Directory to use TLS, you must request and install a certificate on the Active Directory server. The certificate must meet the following requirements:

- Be located in the Local Computer's Personal certificate store. This can be seen using the Certificates MMC snap-in.
- Have the private details on how to obtain a key associated for use with it stored locally. When viewing the certificate you should see a message saying "You have a private key that corresponds to this certificate''.
- Have a private key that does not have strong private key protection enabled. This is an attribute that can be added to a key request.
- The Enhanced Key Usage extension includes the Server Authentication object identifier, again this forms part of the key request.
- Issued by a CA that both the domain controller and the client trust.
- Include the Active Directory fully qualified domain name of the domain controller in the common name in the subject field and/or the DNS entry in the subject alternative name extension.

To configure the VCS to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the VCS by navigating to:

- *Maintenance > Security.*

LDAP Configuration

OpenLDAP

Prerequisites

These instructions assume that an OpenLDAP server has already been installed. For details on installing OpenLDAP see the documentation at http://www.openldap.org.

The following examples use a standard OpenLDAP installation on the Linux platform. For installations on other platforms the location of the OpenLDAP configuration files may be different. See the OpenLDAP installation documentation for details.

Installing the H.350 Schemas

1. Copy the OpenLDAP files to the OpenLDAP schema directory:

```
/etc/openldap/schemas/commobject.ldif
/etc/openldap/schemas/h323identity.ldif
/etc/openldap/schemas/h235identity.ldif
/etc/openldap/schemas/sipidentity.ldif
```

2. Edit `/etc/openldap/slapd.conf` to add the new schemas. You will need to add the following lines:

```
include /etc/openldap/schemas/commobject.ldif
include /etc/openldap/schemas/h323identity.ldif
include /etc/openldap/schemas/h235identity.ldif
include /etc/openldap/schemas/sipidentity.ldif
```

The OpenLDAP daemon (`slapd`) must be restarted for the new schemas to take effect.

Adding H.350 Objects

Create the Organizational Hierarchy

1. Create an `ldif` file with the following contents:

```
# This example creates a single
# organizational unit to contain the H.350
# objects
dn: ou=h350,dc=my-domain,dc=com
objectClass: organizationalUnit
ou: h350
```

2. Add the ldif file to the server using the command:

```
slapadd -l <ldif _ file>
```

This organizational unit will form the BaseDN to which the VCS will issue searches. In this example the BaseDN will be: `ou=h350,dc=my-domain,dc=com`.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the VCS read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 Objects

1. Create an `ldif` file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=my-domain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
```

2. Add the `ldif` file to the server using the command:

```
slapadd -l <ldif _ file>
```

This will add a single H.323 endpoint with an H.323 Id alias of MeetingRoom1 and an E.164 alias of 626262. The entry also has H.235 credentials of id meetingroom1 and password mypassword which are used during authentication.

Securing with TLS

The connection to the LDAP server can be encrypted by enabling Transport Level Security (TLS) on the connection. To do this you must create an X.509 certificate for the LDAP server to allow the VCS to verify the server's identity. Once the certificate has been created you will need to install the following three files associated with the certificate onto the LDAP server:

- The certificate for the LDAP server.
- The private key for the LDAP server.
- The certificate of the Certificate Authority (CA) that was used to sign the LDAP server's certificate.

All three files should be in PEM file format.

The LDAP server must be configured to use the certificate. To do this:

1. Edit `/etc/openldap/slapd.conf` and add the following three lines:

```
TLSCACertificateFile <path to CA certificate>
TLSCertificateFile <path to LDAP server certificate>
TLSCertificateKeyFile <path to LDAP private key>
```

The OpenLDAP daemon (`slapd`) must be restarted for the TLS settings to take effect.

To configure the VCS to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the VCS by navigating to:

- *Maintenance > Security.*

Bibliography

Reference	Title	Link
1	ITU Specification: H.235 Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals	http://www.itu.int/rec/T-REC-H.235/en
2	ITU Specification: H.350 Directory services architecture for multimedia conferencing	http://www.itu.int/rec/T-REC-H.350/en
3	RFC 2782: A DNS RR for specifying the location of services (DNS SRV)	http://www.ietf.org/rfc/rfc2782.txt
4	RFC 3164: The BSD syslog Protocol	http://www.ietf.org/rfc/rfc3164.txt
5	RFC 3880: Call Processing Language (CPL): A Language for User Control of Internet Telephony Services	http://www.ietf.org/rfc/rfc3880.txt
6	DNS and BIND Fourth Edition, Albitz and Liu, O'Reilly and Associates, ISBN: 0-596-00158-4	
7	RFC 2915: The Naming Authority Pointer (NAPTR) DNS Resource Record	http://www.ietf.org/rfc/rfc2915.txt
8	RFC 3761: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)	http://www.ietf.org/rfc/rfc3761.txt
9	Mastering Regular Expressions, Jeffrey E.F. Friedl, O'Reilly and Associates, ISBN: 1-56592-257-3	
10	RFC 3327: Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts	http://www.ietf.org/rfc/rfc3327.txt
11	Session Traversal Utilities for (NAT) (STUN)	http://www.ietf.org/internet-drafts/draft-ietf-behave-rfc3489bis-06.txt
12	Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN)	http://www.ietf.org/internet-drafts/draft-ietf-behave-turn-03.txt
13	RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP	http://www.ietf.org/rfc/rfc4787.txt
14	RFC 4028: Session Timers in the Session Initiation Protocol (SIP)	http://www.ietf.org/rfc/rfc4028.txt
15	ITU Specification: H.323: Packet-based multimedia communications systems	http://www.itu.int/rec/T-REC-H.323/en
16	RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers	http://www.ietf.org/rfc/rfc3263.txt
17	RFC 3550: RTP: A Transport Protocol for Real-Time Applications	http://www.ietf.org/rfc/rfc3550.txt
18	RFC 791: Internet Protocol	http://www.ietf.org/rfc/rfc791.txt
19	RFC 2460: Internet Protocol, Version 6 (IPv6) Specification	http://www.ietf.org/rfc/rfc2460.txt
20	RFC 3261: SIP: Session Initiation Protocol	http://www.ietf.org/rfc/rfc3261.txt
21	RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)	http://www.ietf.org/rfc/rfc3489.txt

Glossary

Term	Definition
A record	A type of DNS record that maps a domain name to an IPv4 address.
AAAA record	A type of DNS record that maps a domain name to an IPv6 address.
Administrator Policy	In relation to the VCS, the set of rules configured system-wide (either via the web interface or CPL script) that determine the action(s) to be applied to calls matching a given criteria.
Alias	The name an endpoint uses when registering with the VCS. Other endpoints can then use this name to call it.
Alternate	One or more VCSs configured to support the same zone in order to provide redundancy.
ARQ Admission Request	An endpoint RAS request to make or answer a call.
Assent	TANDBERG's proprietary protocol for firewall traversal.
Border Controller	A TANDBERG device used to control multimedia networks and firewall traversal.
Call Policy	The set of rules (administrator policy, user policy and transforms) that are applied to a single call to determine whether and how it is placed.
CLI Command Line Interface	A text-based user interface used to access the VCS.
CPL Call Processing Language	An XML-based language for defining call handling. Defined by RFC 3880 [5].
DNS Domain Name System	A distributed database linking domain names to IP addresses.
DNS zone	On the VCS, a zone used to configure access to endpoints located via a DNS lookup.
E.164	An ITU standard for structured telephone numbers. Each telephone number consists of a country code, area code and subscriber number. For example, TANDBERG's European Headquarters' phone number is +47 67 125125, corresponding to a country code of 47 for Norway, area code of 67 for Lysaker and finally 125125 to determine which phone line in Lysaker.
ENUM tElephone NUmber Mapping	A means of mapping E.164 numbers to URIs using DNS.
ENUM zone	On the VCS, a zone used to configure access to endpoints located via ENUM.
External Manager	The remote system that is used to manage endpoints and network infrastructure. The TANDBERG Management Suite (TMS) is an example of an external manager.
Firewall traversal	Crossing a firewall or NAT device.
FindMe™	A TANDBERG feature that allows users to have a single alias on which they can be reached regardless of the endpoint(s) they are currently using.
FQDN Fully Qualified Domain Name	A domain name that specifies the node's position in the DNS tree absolutely, uniquely identifying the system or device.
Gatekeeper	A device used to control H.323 multimedia networks. An example is the TANDBERG Gatekeeper.
Gatekeeper Zone	A collection of all the endpoints, gateways and MCUs managed by a single gatekeeper.
H.323	A standard that defines the protocols used for packet-based multimedia communications systems.
HTTP Hypertext Transfer Protocol	A protocol used for communications over the internet.
HTTPS	A protocol used for secure communications over the internet, combining HTTP with TLS.
Hop count	The number of times a location request may be forwarded to a gatekeeper or proxy before it is deemed to have failed.
ICE Interactive Connectivity Establishment	A collaborative algorithm that works together with STUN services (and other NAT traversal techniques) to allow clients to achieve firewall traversal.
IETF Internet Engineering Task Force	An organization that defines (via documents such as RFCs) the protocol standards and best practices relating to the design, use and management of the internet.

Term	Definition
Interworking	Allowing H.323 systems to connect to SIP systems.
IPv4 Internet Protocol version 4	Version 4 of the Internet Protocol, defined in RFC 791 [18].
IPv6 Internet Protocol version 6	Version 6 of the Internet Protocol, defined in RFC 2460 [19].
IRQ Information Request	A request sent to an endpoint requesting information about its status.
LAN Local Area Network	A geographically limited computer network, usually with a high bandwidth throughput.
LDAP Lightweight Directory Access Protocol	A protocol for accessing on-line directories running over TCP/IP.
Link	In relation to the VCS, a connection between two nodes.
LRQ Location Request	A RAS query between gatekeepers to determine the location of an endpoint.
NAPTR record	A type of DNS record.
NAT Network Address Translation	Also known as IP masquerading. Rewriting source and destination addresses as the IP packet passes through the NAT device.
Node	In relation to the VCS, a node is one end of a link. A node can be a local subzone or a zone.
NTP Network Time Protocol	A protocol used for synchronizing clocks.
Pipe	In relation to the VCS, a means of controlling the bandwidth used on a link.
Proxy, Proxy Server	In SIP, an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity “closer” to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it. While a proxy can set up calls between SIP endpoints, it does not participate in the call once it is set up.
RAS Registration, Admission and Status	A protocol used between H.323 endpoints and a gatekeeper to register and place calls.
Registrar	In SIP, a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles. This information is used to advise other SIP Proxies/Registrars where to send calls for that endpoint.
Regex Regular Expression	A pattern used to match text strings according to a POSIX-defined syntax.
RFC Request for Comments	A process and result used by the IETF for Internet standards.
RS-232	A commonly used standard for computer serial ports.
RTCP RTP Control Protocol	A control protocol for RTP, defined by RFC 3550 [17].
RTP Real-time Transport Protocol	Real time protocol designed for the transmission of voice and video. Defined by RFC 3550 [17].
SSH Secure Shell	An encrypted protocol used to provide a secure CLI.

Term	Definition
SIP Session Initiation Protocol	IETF protocol for controlling multimedia communication. Defined by RFC 3261 [20]
SNMP Simple Network Management Protocol	A protocol used to monitor network devices.
Source Alias	The alias present in the “source” field of a message.
SRV record Service record	A type of DNS record.
STUN Simple Traversal of UDP through NATs	Firewall NAT traversal for SIP. Defined by RFC 3489 [21].
Subzone	A segment of a VCS zone.
TCP Transmission Control Protocol	A reliable communication protocol defined by RFC 791 [18].
Telnet	A network protocol used on the internet or Local Area Networks (LANs).
TLS Transport Layer Security	A protocol that provides secure communications over the internet.
Transform	In relation to the VCS, the process of changing the alias being searched for.
Traversal call	Any call where both signaling and media are routed through the VCS.
Traversal Client	A traversal entity on the private side of a firewall. Examples are a TANDBERG Gatekeeper or TANDBERG VCS.
Traversal Server	A traversal entity on the public side of a firewall. Examples are the TANDBERG Border Controller and the TANDBERG VCS with the Border Controller option enabled.
Traversal-enabled endpoint	Any endpoint that supports the Assent and/or ITU H.460.18 and H.460.19 standards for firewall traversal. This includes all TANDBERG MXP endpoints.
UDP User Datagram Protocol	Unreliable communication protocol defined by RFC 791 [18].
URI Uniform Resource Identifier	A formatted string used to identify a resource, typically on the internet.
User Policy	The set of rules that determine the action(s) to be applied to calls for a particular user or group.
VCS Border Controller	A VCS with the Border Controller option added. This allows the VCS to act as a firewall traversal server.
Zone	A collection of endpoints.

TANDBERG

Philip Pedersens vei 22, 1366 Lysaker, Norway
Telephone: +47 67 125 125
Fax: +47 67 125 234
Video: +47 67 117 777
E-mail: tandberg@tandberg.com